

# Datafox ZK-MasterIV



Access only for authorized persons

## Contents

<b>1</b>	<b>Introduction</b>	<b>7</b>
1.1	Updates in this document	7
1.2	Alterations of the version	7
1.3	The device file archive (*.dfz)	7
1.3.1	Description	7
1.3.2	Function of the archive	7
1.3.3	Manual selection of a file	7
1.4	Typography of the manual	8
1.5	Important general advice	9
<b>2</b>	<b>System structure and functional principle</b>	<b>11</b>
2.1	Software versions and compatibility of device firmware and setup	11
2.2	Firmware	13
2.2.1	Firmware update	13
2.2.2	Firmware downgrade	13
2.3	System structure	14
2.3.1	Device functions	14
2.3.2	Communication	14
<b>3</b>	<b>ZK-MasterIV</b>	<b>18</b>
3.1	Technical data	18
3.2	Connection	19
3.2.1	Power supply	22
3.2.2	Digital Input	22
3.2.3	USB connector	23
3.2.4	Ethernet interface	23
3.2.5	Mobile communications modem	23
3.3	Commissioning	24
3.4	Operation	24
3.5	Communications	24
3.5.1	Communication via RS232	24
3.5.1.1	Requirement	24
3.5.1.2	Connection	24
3.5.1.3	Conversion of RS232 to RS485	25
3.5.2	Communication via USB	27
3.5.2.1	Conditions	27
3.5.2.2	Connection	27
3.5.2.3	Driver installation	27
3.5.2.4	USB stick as data medium	30
3.5.2.4.1	Data structure and security	30
3.5.2.4.2	Change the password of the communication	33
3.5.3	Communication via analogous modem	34
3.5.3.1	Conditions	34
3.5.3.2	Connection	34
3.5.3.3	Modem initialization	37
3.5.3.4	Connection via the DatafoxStudioIV	37
3.5.3.5	Connection via the DFComDLL	38
3.5.4	Communication via GSM or GPRS/GSM	39
3.5.4.1	Preparation	39

3.5.4.2	Configuration	39
3.5.4.3	Connection state	40
3.5.4.4	Send data via GPRS	41
3.5.5	Communication via TCP/IP	43
3.5.5.1	LAN	44
3.5.5.2	Transition from TCP/IP to RS232	45
3.5.5.3	Transition from TCP/IP to RS485 Bus	46
3.5.5.4	WLAN	47
3.5.6	Communication via RS485	47
3.5.7	Active connection via TCP/IP	48
3.5.7.1	Description	48
3.5.7.2	Configuration of an active connection	49
3.5.7.3	Device servicing via active connection	51
3.5.8	WLAN	53
3.5.8.1	General information	53
3.5.8.2	Terms and explanations	53
3.5.8.2.1	Infrastructure Mode	53
3.5.8.2.2	Ad-hoc Mode	53
3.5.8.2.3	Frequencies and ports	54
3.5.8.2.4	Security and encryption	54
3.5.8.2.5	Authentication	54
3.5.8.2.6	Passwords	55
3.5.8.3	BIOS dialogue DatafoxStudioIV	55
3.5.8.4	Dependencies	56
3.5.8.5	WLAN configuration via the Lantronix tool	56
3.5.8.6	WLAN configuration via the DatafoxStudioIV	57
3.5.8.6.1	General	57
3.5.8.6.2	Selection of the serial interface	57
3.5.8.6.3	Selection of the configuration file	58
3.5.8.6.4	TCP/IP settings	59
3.5.8.6.5	WLAN settings	59
3.6	Access control II with TS TMR33 modules	61
3.6.1	Set-up	61
3.6.1.1	A door without a separate reader	62
3.6.1.2	A door with a separate reader	62
3.6.1.3	Several external doors via RS485 bus	63
3.6.1.4	Several internal doors via RS485 bus	64
3.6.1.5	Mantrap function with RS485 bus	65
3.6.2	Connection	66
3.6.2.1	Wiring	67
3.6.2.2	Calculation instructions	73
3.6.2.3	Topologie	74
3.6.2.4	Examples	74
3.6.2.4.1	Bus topology	74
3.6.2.4.2	Star topology	75
3.6.3	Configuration	76
3.6.4	An example for a ZK system	80
3.7	Timing of the digital exits for the MasterIV device series	86
3.8	Access control II with PHG modules	88
3.8.1	Connection	89

3.8.2	Configuration	90
3.9	Status message of the access control	91
<b>4</b>	<b>DatafoxStudioIV - General operation</b>	<b>93</b>
4.1	Installation	93
4.2	Operation of the DatafoxStudioIV	93
4.3	Menu Datei	94
4.3.1	Creating a new setup file	94
4.3.2	Open setup file	95
4.4	Menu Setup	96
4.4.1	Edit	96
4.4.2	Import access control lists	96
4.4.3	Configure data storage	97
4.4.4	Load firmware	98
4.4.5	Device maintenance via modem connection	99
4.4.5.1	Functions for device maintenance	100
4.4.6	Edit text data of the firmware	102
4.5	Menu Communication	105
4.5.1	Write / read setup	105
4.5.2	Load lists/ access control lists	105
4.5.3	Import and load Timeboy lists	106
4.5.4	Read, delete, display data	107
4.5.4.1	Read data and delete them	107
4.5.5	Set time	107
4.5.6	Read serial number	107
4.5.7	Read global variables	108
4.5.8	System variables of the signal processing	109
4.5.9	Display state of the ZK-modules	110
4.5.10	Work through batches	111
4.5.11	GPRS configuration	112
4.5.12	Device configuration BIOS	114
4.5.13	Settings	117
4.6	Menu Extra	119
<b>5</b>	<b>DatafoxStudioIV - Setup</b>	<b>120</b>
5.1	Basics	120
5.1.1	Planning	120
5.2	Functions of a setup	122
5.2.1	Basic settings	122
5.2.2	Global variables	122
5.2.3	Transponder	123
5.2.3.1	Transponder reading systems	125
5.2.3.2	Function upgrading for Mifare transponders	131
5.2.3.2.1	General information	131
5.2.3.2.2	Global settings	131
5.2.3.2.3	Function normal	134
5.2.3.2.4	Transponder value write, also for Hitag1, Hitag2 and Titan	134
5.2.3.2.5	Transponder menu	134
5.2.3.3	Application possibilities for Hitag-transponder	135
5.2.4	Creating data record descriptions	137
5.2.5	Creating list descriptions	138

5.2.6	Creating a user guidance . . . . .	139
5.2.6.1	Defining input chains . . . . .	139
5.2.6.2	Defining input fields . . . . .	140
5.2.6.2.1	Field functions in general . . . . .	141
5.2.6.2.2	Field functions of the access control . . . . .	142
5.2.6.3	Expanded . . . . .	142
5.2.6.4	Reaction on list selection . . . . .	143
5.2.6.5	Jumps . . . . .	143
5.2.7	Signal processing . . . . .	143
5.2.7.1	Use as Start/Stop . . . . .	143
5.2.7.2	Use as counter . . . . .	144
5.2.7.3	Use as counter with Start/Stop . . . . .	145
5.2.7.4	Use as counter with Start/Stop via timeout . . . . .	145
5.2.7.5	Use as counter with Start/Stop via timeout and 1st counting impulse . . . . .	146
5.2.7.6	Connection Timeboy . . . . .	147
5.2.7.7	Alive data record . . . . .	147
5.2.7.8	Setting of timers . . . . .	147
5.2.7.9	Setting of timers . . . . .	147
5.2.8	Mathematical operations . . . . .	147
5.3	Creating setups . . . . .	149
5.3.1	Setup for access control version II . . . . .	149
5.3.1.1	General . . . . .	149
5.3.1.2	Hardware components of access control system . . . . .	149
5.3.1.3	Basic settings . . . . .	150
5.3.1.4	Creating a data record description . . . . .	151
5.3.1.5	Creating the access control lists . . . . .	152
5.3.1.6	Creating an input chain of access control . . . . .	154
5.3.1.7	Transmission of the complete configuration to the terminal . . . . .	157

© 2008 by Datafox GmbH

This document has been created by Datafox GmbH and is copyrighted against third parties. Datafox GmbH considers all contained information, knowledge and depictions as its sole property. All rights, including also translation, reprint or copy of the whole document or parts of it, require written consent of Datafox GmbH. The assertion of all rights in this respect is reserved to Datafox GmbH, especially in case of the grant of a patent. The handover of this documentation does not establish a claim to the licence or the use the soft- and hardware. Copies of the diskettes and CDs may only be made for the purpose of data backup. Every unauthorized copy of this documentation or the Datafox-software will be prosecuted.

## 1 Introduction

### 1.1 Updates in this document

### 1.2 Alterations of the version

With the device generation IV a new versioning scheme has been introduced. According to this scheme the file name of the device firmware and the setup program (DatafoxStudioIV) is composed as follows:

product name	XX. device- generation	YY. compatibility (which versions can be used together)	ZZ. version number (functional ex- tension)	Build Build trou- bleshooting (with a new ver- sion the Build number is reset)
e. g. ZK-MasterIV	04.	01.	01.	12

The use of the manual depends on the version of the firmware and the DatafoxStudioIV or the DFComDLL. Gather from the following table which manual matches which version. For different combinations no support can be offered.

date	version			
	manual	firmware	Studio/DLL	description
21. Dez. 2006	4.01.03	4.01.03	4.01.03	new release
06. Juni 2007	4.01.04.16	4.01.04.16	4.01.04.16	new release

### 1.3 The device file archive (\*.dfz)

#### 1.3.1 Description

Device files (\*.hex) of the MasterIV - devices are delivered in a common device file archive. It has the file extension dfz (stands for Datafox Zip). Now simply the device file archives are indicated instead of the device files (\*.hex). This applies to the DatafoxStudioIV and DLL. The indication of device files (\*.hex) is still possible.

#### 1.3.2 Function of the archive

The transmission routine of the device file picks out the fitting file from the device file archive on the basis of the hardware options available in the device. Thus, it is guaranteed that all hardware components available in the device are supported by the corresponding firmware.

#### 1.3.3 Manual selection of a file

If you do not want to integrate the archive in your installation, you have the possibility to add single device files from the archive to the installation.

The file format of the device file archive is Zip. Hence, you can open the archive with every standard Zip-program. Via the menu item "open with..." in the context menu you can chose an appropriate program

for opening the file. If necessary you can call up a program combined with this file format to open the file by renaming the file from dfz to zip.

In the archive you find a file called Inhalt.pdf; you can gather from there which file (\*.hex) of the archive matches your device. Extract the device file (\*.hex) you want and rename it if necessary. A renaming of a file is always possible, because all information are in the file itself.

You can state the device file extracted before as device file in DatafoxStudioIV and at calling the DLL function. It is still tested if the file can be loaded into the chosen device before the transmission takes place.

## 1.4 Typography of the manual

### exposition

### contextual meaning

< *ZK-MasterIV, SoftwareVersion.pdf* >

file names

< *Setup => edit* >

a path via a program menu at DatafoxStudioIV

*communication*

a single menu item

FW

abbreviation for firmware (software in the device)

(from FW V 3.1.5)

shows that this function is supported from the firmware version 3.1.5 onwards

SW

abbreviation for software

HW

abbreviation for hardware

(from HW V 2.0)

shows that this option is available from the hardware version 2.0 onwards

GV

abbreviation for global variable

ZK-list

abbreviation for access control lists, where the configuration data for the access control is provided

cross-reference [1.4](#)

In the electronic document you can use the cross-references to jump within the manual. Therefore, cross-references are depicted in blue and crossing them the cursor takes the shape of a hand .



#### Note:

You will get useful advice which helps you to avoid possible mistakes during the installation, configuration and commissioning.





**Caution:**

There will be advice given you definitely have to keep to. Otherwise it will lead to defective function of the system.

### 1.5 Important general advice



**Caution:**

Use the devices only according to regulations and following the assembly, commissioning and operating instructions. Assembly and commissioning may only be carried out by authorized and qualified personnel.

#### Subject to technical alterations.



**Caution:**

Because of technical development illustrations, functional steps, technical processes and data can differ slightly.

Datafox ZK-MasterIV has been developed to create a flexible terminal for time and attendance, order time collection and access control that can easily be integrated. The device is robust and easy to use. You save time through the PC - setup program, because the device is quickly and easily configured for its application field.

#### **This manual describes the creation of work flows for time and attendance with the setup program.**

Before deciding for the programming in C you should check if the functions of the setup program do fulfil the system requirements after all , because then the development effort will be reduced to a minimum. With some exercise it will be possible to compile a complete entry within half an hour. If you need functions that are not available we should get into contact.

If you need support at the compilation of setups we offer you our services. Because of our wide experience in dealing with the setup we are very quick and can make your setup even more efficient through useful advice, so that the entry at the device can take place quickly and reliably.

Through our experience and with our specialized knowledge of method, hard- and software we produce devices and find solutions concerning data collection, that prove themselves with functionality and practicality. We offer solutions for REFA/ job analysis, time and attendance, production data collection, machine data collection, process data collection and mobile data collection. Our team develops and produces standardized and inexpensive systems. We create solutions using the modular principle and expand them as required. Our service includes consultation, system definition and implementation as well as workshops and training to support you in the introduction.

#### **Guarantee restriction**

All data in this manual has been checked carefully. Nevertheless, errors cannot be excluded. Therefore, there cannot be given guarantee nor taken legal responsibility for consequences that derive from errors of this manual. Of course we are grateful if you point out errors to us. Subject to change because of technical improvements. Our general terms and conditions of business apply.



**Note:**

Because of the DatafoxStudioIV the Datafox devices have many functions and combination of functions; therefore, it is not possible to test all functions and their combinations in case of updates. This applies especially to all the setups you created as a customer. Before updating your device please test if your individual setup works without errors. If you detect an error contact us immediately. We will rectify the mistake at short notice.

## 2 System structure and functional principle

### 2.1 Software versions and compatibility of device firmware and setup

The firmware (operating system) of the device and the setup program (\*.aes data file = application program) form a unit. With the setup program the configuration for the device (definition of the data tables and the data fields, operation, etc.) is compiled and transmitted to the device. Then the firmware works in accordance with the setup adjustments.

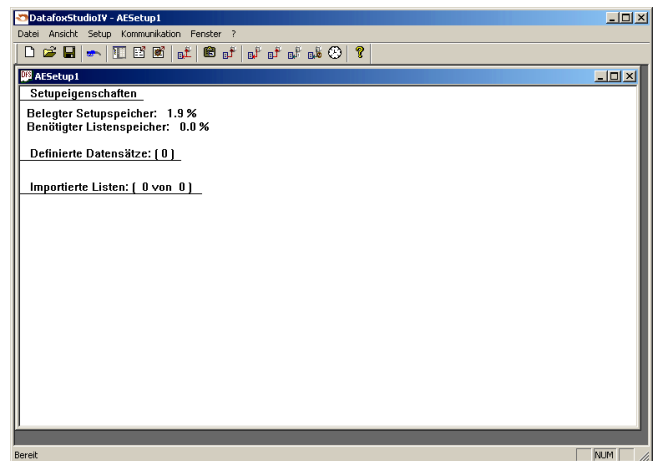
#### Firmware in device



After switching-on the current firmware version is shown on the display. The firmware can be transmitted to the device with DatafoxStudioIV.

At delivery a demo setup is at the device. The description of the demo setup you will find in chapter 5.3.1. It is advisable to go through the example at first comparing the process with the setup. That way a quick introduction to the configuration is possible.

#### Setup program on PC



After starting the setup program the user interface is displayed.

You can get information about the current software version via the info dialog of DatafoxStudioIV. Click on the < ? > in the menu bar and then on < info over DatafoxStudioIV >..



## Compatibility of firmware and DatafoxStudioIV

The DatafoxStudioIV is downward compatible within the firmware versions 4.x.xx. The second number shows the compatibility group. If this number is changed, a more up-to-date firmware generation must be used.



### Note:

Devices with an older firmware can also be configured with DatafoxStudioIV, but only that functions are provided by the device which are also provided by the older firmware. However, it is impossible to configure a more up-to-date firmware version with an older DatafoxStudioIV-Version.

That means, the manual version that corresponds to the firmware with the appropriate setup is always relevant for the possible functions. The manual version and the appropriate DatafoxStudioIV always have the same index. It is impossible to configure a firmware with a DatafoxStudioIV version that is older than the firmware. Recommendation: If possible use the appropriate DatafoxStudioIV version. This version always has to be  $\geq$  the version of the firmware.

### The data file:

< ZK – MasterIV, SoftwareVersionen Stand xxx.pdf > shows which functions are provided by which software release. You will find the file on the CD. Please also comply with the instructions given in the chapters of the manual.

The updates are available for download on our internet page [www.datafox.de](http://www.datafox.de).



### Caution:

When the new device is delivered always the firmware version recently released is used. If you wish to work with an older version please carry out a downgrade. Please comply with the instructions in chapter 2.2.2.

## 2.2 Firmware



**Caution:**

A firmware update or downgrade is a very sensitive process. Possibly a reset of the main communication to RS232 may occur. In any case comply with the details about the compatibility in the software version list.

### 2.2.1 Firmware update



**Caution:**

Before starting a firmware update please check on the basis of the software version list whether there are any version dependencies that must be kept.

For example, when changing from version 04.00.xx to version 04.01.xx there must be a version 04.00.23.769 or higher as minimum requirement to carry out the update to version 04.01.xx successfully.

### 2.2.2 Firmware downgrade



**Caution:**

When carrying out a firmware downgrade the firmware always has to be transmitted to the device twice. This has technical reasons. Errors on the display of the device after the first transmission can be ignored.

## 2.3 System structure

### 2.3.1 Device functions

In principle, Datafox ZK-MasterIV offers two possibilities to create workflows for data collection.

- ▶ Via the PC-setup program "DatafoxStudioIV" many processes for data collection can be created quickly without programming knowledge. Such a process is a setup for the device and can be loaded on the device via the communication program. Devices using such setup programs are equipped with the standard firmware at production. (Details about the software versions see chapter 2.1)
- ▶ Free Programming in C. The progression packet offers many basis routines and a supporting program which can be used as basis for own programs. Devices for c-programming are delivered without the standard firmware and only in connection with an instruction.

### 2.3.2 Communication

There are 4 possibilities available for communication/ data transmission.

#### 1.) Setup- and communication program

The setup- and communication program supports both the setting of the device settings and the important possibilities of data transmission (these data transmission functions are for test purposes primarily). Of course they can also be used for regular data transmission. But this is disadvantageous, because 2 work steps are necessary: At first you have to read out the data via the setup- and communication program and to file them as ASCII-file. Then the second program has to be opened and the file must be imported.

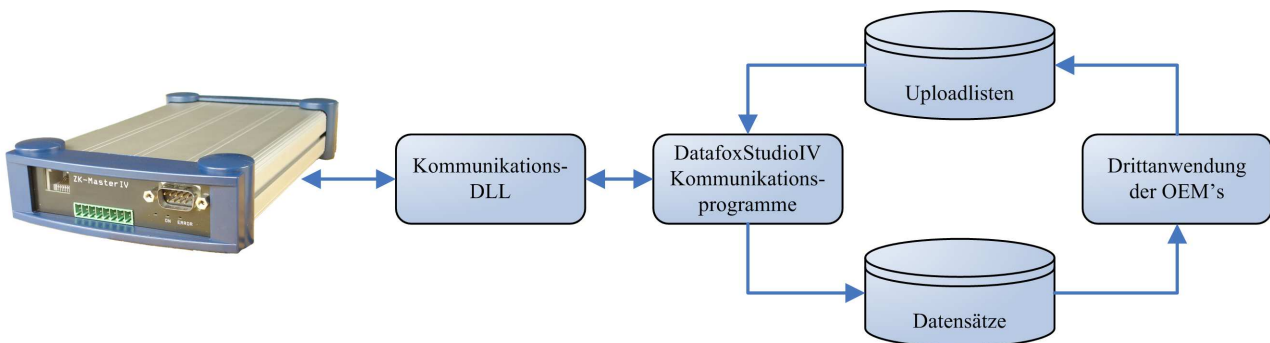


Figure 1: Setup- and Communication programm

2.) **Communication DLL**

The direct way for communicating with the ... is the communication DLL. It can be started with any Windows application. The whole process can be realized without any intermediate files and also be set individually. We advise software producers to choose this method for the integration of the devices. You can find the DLL and the appropriate explanation on the installing-CD.

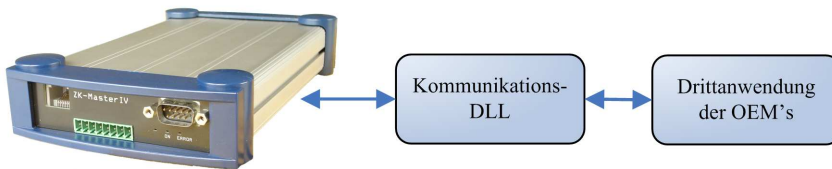


Figure 2: Communication-DLL

3.) **Direct integration via C-Source code**

There are some operating systems that do not support the use of DLLs. In order to solve this problem there is also a C-Source code available on the installing-CD. That way communicating with programs designed under Unix or Linux is also possible.

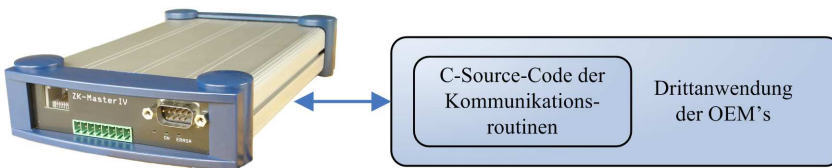


Figure 3: Implementation via C-Sourcecode

4.) **Datafox-Talk**

Via Datafox-Talk data transmission with Datafox AEIII+, Timeboy and the MasterIV-series is possible on file- and database layer. Therefore it is an alternative to communication via DLL. An advantage of this method is, that no installation is necessary. The data are taken over and displayed as ASCII-file. If desired and with computation a direct connection to databases is possible. There the costumer has to decide which database tables and fields shall be filled. Datafox-Talk supports all functions for transmitting data and for setting the device. Via timing the times for transmission can be set freely. Via additional modules the data can also be transmitted per radio, internet, telephone-/ mobile network.

**Advantages:**

- ▶ Via Datafox-Talk integration of the devices can be realized easily and fast.
- ▶ Transmission takes place automatically and is ensured via a log file.
- ▶ The data are accessible forthwith.
- ▶ There is no programming work for data transmission.

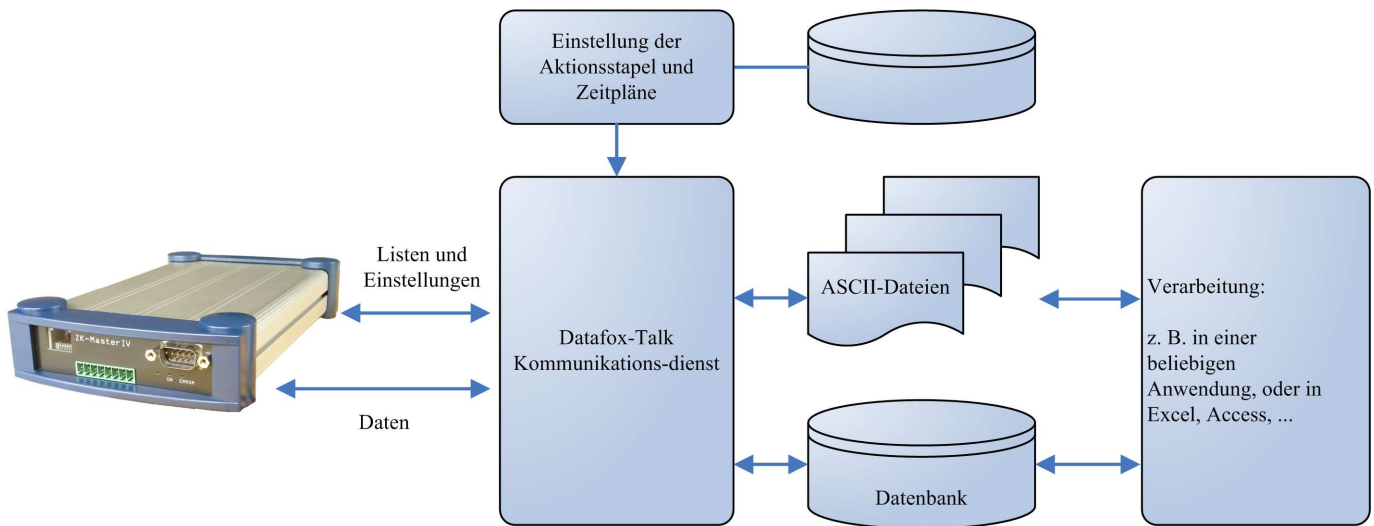


Figure 4: Datafox-Talk

**Supports the following types of transmission:**

- ▶ RS232
- ▶ RS485
- ▶ TCP/IP
- ▶ WLAN
- ▶ Funk 433 MHz
- ▶ Modem (GSM/GPRS)
- ▶ Cellular radio, mobile phone with integrated modem

**The following actions are possible:**

- ▶ Transmitting setup to the devices
- ▶ Setting a clock
- ▶ Transmitting lists to the devices
- ▶ Reading out of data
- ▶ Writing log files and error lists where necessary
- ▶ Filing of data as ASCII-file, Excel-file, Dbase-File or ACCESS-database

The actions are applied as batch and carried out according to the settings of the timing. Timing allows the permanent collection of data (polling) and the collection at any time. The setting via time model is very easy. The working through the actions is logged and therefore always traceable. The same applies to the transmission of lists. Lists are used e.g. to back-up applications, accounts, occupations etc. or to transmit balances.



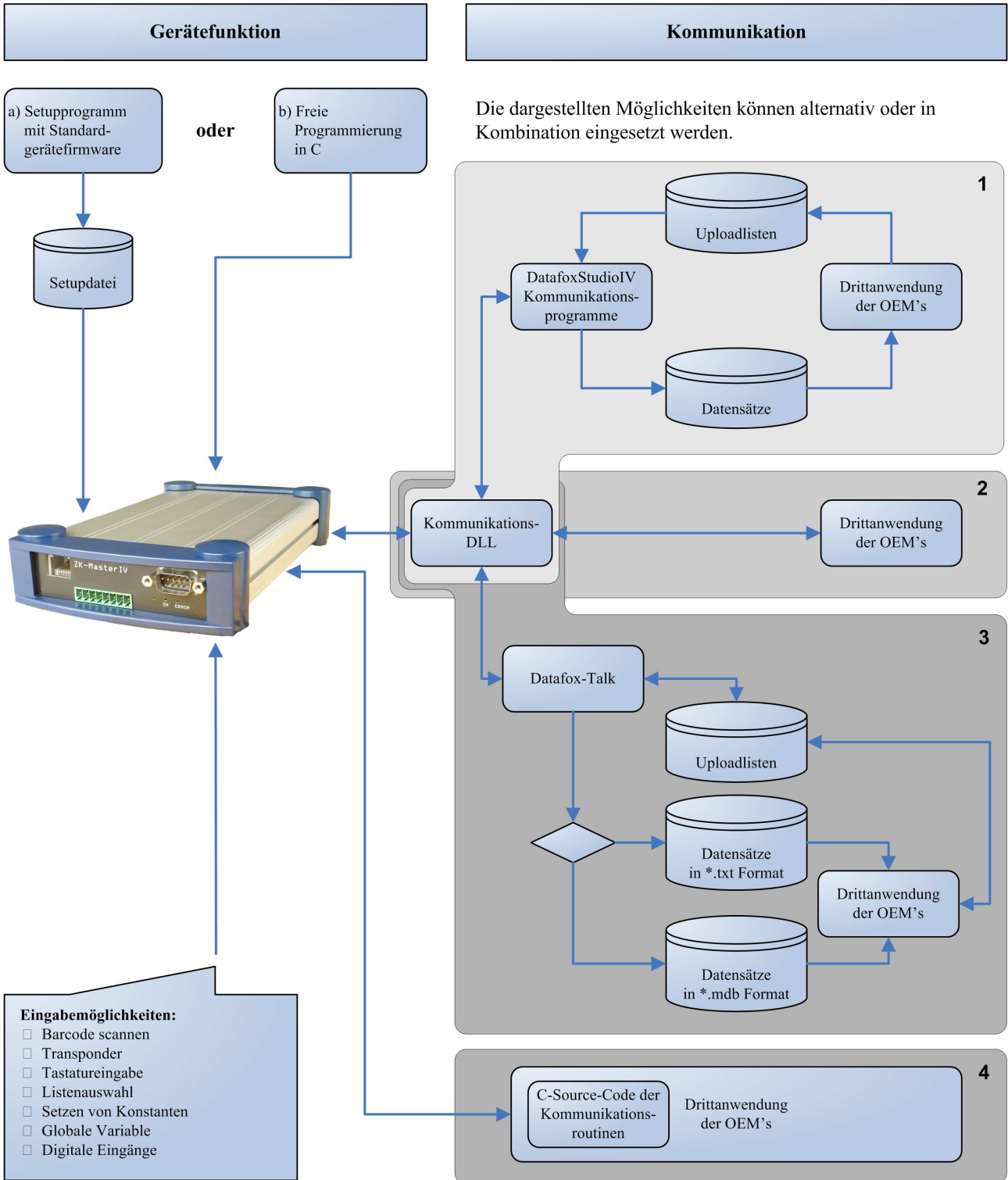


Figure 5: System structure

### 3 ZK-MasterIV

When using the ZK-MasterIV you have to comply with the temperature range of -20 to +70°C, see data sheet.

!

**Caution:**

Plas keep in mind that MasterIV terminals use a flash memory. According to the manufacturer each memory sector (512 byte) can be written to a maximum of 100,000 times. The firmware of the terminals distributes the access to the memory sectors, this technique is called wear levelling. Bad blocks in case of write or read failures are not used anymore. However, despite this technique it is not advisable to write the memory too frequently. The application should initialize a new list transfer only after a change of the list data but not cyclically.

Keep in mind the message - FlashService - in the display of the device. It means that the live time of the flash memory according to the manufacturer instruction will be reached soon. Then the device has to be sent to Datafox for service.

#### 3.1 Technical data

<b>CPU</b>	Controllor	8 bit, 16 MHz
	Clock	real-time-clock
<b>Program memory</b>	Flash	128 Kbyte
<b>Data memory</b>	Flash	2 MB Defaul
	Memory extension	Multi-Media-Card(MMC) up to 1 GB Flash
<b>Power supply</b>	Power supply	24 volts of change tension or DC voltage
	Lithium battery	care of the clock with stream failure
<b>Power consumption</b>	Maximal	7,2 Watt
	Basicdevice	4 Watt
<b>Dimensions</b>	length x width x depth	205mm x 120mm x 40mm
<b>Weight</b>	Without power supply	400 g
<b>Environment factors</b>	Environmental temerature	-20 to +70 °C
	Protection class	IP 40
<b>Software</b>	Configuration program	Setup program for arrangement witout programming
	Communication tools	Communication-DLL
<b>Data transfer</b>	RS232 /RS485	RS232 und RS485 in basic unit
	TCP-IP (option)	TCP/IP use via integrated TCP/IP stack
	WLAN (option)	Wireless LAN via external ACCESS-Point
	GSM/GPRS (option)	mobile network via GSM and GPRS = online on internet
	Bluetooth (option)	bluetooth module integrated. Up to 100 meters.
<b>Reader connection</b>	RS232 external	connection from cash code reader , magnet card reader et
<b>Access options</b>	RS485 extern	Anschluß von bis zu 8 externen Door module/access reader
	door opener-relay	1 door opener-relay 42 Volt
	digital input	1x door supervision
<b>Options</b>	Transponder reader external	Unique EM4102, Hitag, Legic, Mifare, SimonsVoss
	Säule	Säule für freies Aufstellen

Table 1: Technical data of the ZK-MasterIV HW-Version 2 Subject to technical alterations.

### 3.2 Connection

The ZK-MasterIV (central controller for access control, door- or rather remote control) has to be installed in a safe area which is accessible only for authorized persons. You find the connections of the device narrow sided over the edge connector. That way the installation of the device is easier.



Figure 6: ZK-MasterIV

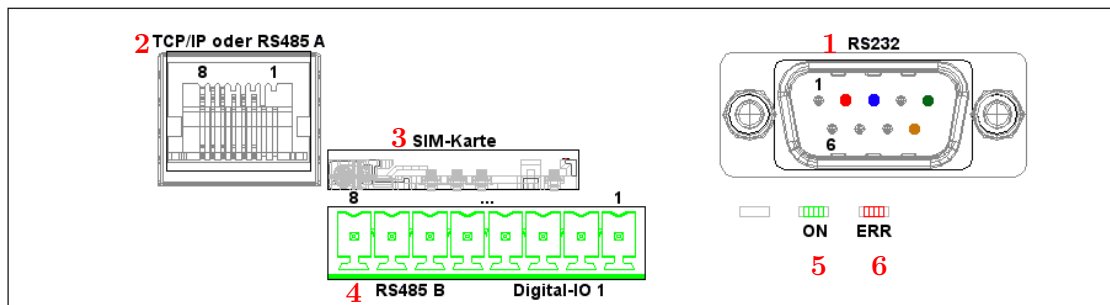


Figure 7: Edge connector of the ZK-MasterIV from HW V 1.4

Designation	Plug	Pin	Description
Power supply	4	5,8	12 V 3 A DC
Digital input (this are potential-free inputs)	4	3	Input 10 Hz 0 - 3 Volt = logical 0 ( $V_{ILmax} = 3,0 \text{ V}$ ) 12-30 Volt = logical 1 ( $V_{IHmin} = 12,0 \text{ V}$ )
		4	GND
Digital output	4	1	common (max. 2,0 A bei 42 V AC or 30 V DC)
		2	Normally-open (Contact)
RS232 interface D-Sub 9 pole	1	2	TxD
		3	RxD
		5	GND
RS485 interface	2	1	24 V DC
		2	GND
		3	Data channel B
		4	Data channel B
		5	Data channel A
		6	Data channel A
RS485 interface of the access control	4	5	GND
		6	Data channel A
		7	Data channel B
		8	12 V DC

Table 2: Overview over connections with pin assignment HW V 1.4

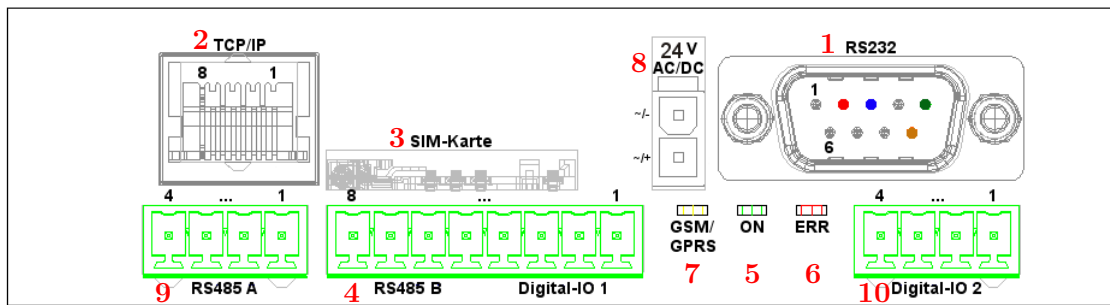


Figure 8: Steckerleiste des ZK-MasterIV ab HW V 2.0

Designation	Plug	Pin	Description
Power supply	8		24 V 300 mA AC/DC (If a DC voltage is connected, the polarity is to be followed.)
Digital input (this are potential-free inputs)	4	3	Input 5 kHz 0 - 1 Volt = logical 0 ( $V_{ILmax} = 1,0 \text{ V}$ ) 3,5 - 30 Volt = logical 1 ( $V_{IHmin} = 3,5 \text{ V}$ )
		4	GND
	10	3	Input 10 Hz 0 - 3 Volt = logical 0 ( $V_{ILmax} = 3,0 \text{ V}$ ) 12-30 Volt = logical 1 ( $V_{IHmin} = 12,0 \text{ V}$ )
		4	GND
Digital output	4	1	common (max. 2,0 A bei 42 V AC or 30 V DC)
		2	Normally-open (Contact)
	10	1	common (max. 2,0 A bei 42 V AC or 30 V DC)
		2	Normally-open (Contact)
RS232 interface D-Sub 9 pole	1	2	TxD
		3	RxD
		5	GND
RS485 interface	9	1	GND
		2	Data channel A
		3	Data channel B
		4	24 V DC
RS485 interface of the access control	4	5	GND
		6	Data channel A
		7	Data channel B
		8	12 V DC

Table 3: Overview over connections with pin assignment HW V 2.0

### 3.2.1 Power supply

The power supply for the ZK-MasterIV (HW V 1.4) is connected to the Datafox device power supply unit 12 V 3 A DC via the 8 pole strip terminal, position (4) in figure 7. From HW V 2.0 on the terminal is supplied with power (24 V 300 mA power supply unit) via the Molex connector (8) in figure 8.

!

**Caution:**

In principle, only one voltage source may be connected to the ZK-MasterIV. Only a 12 V/3 A DC voltage source may be connected to the ZK-MasterIV with HW V 1.4. The terminal and the entire access control-net (16 modules at most) can be energized by this voltage source. You have to connect a 24 V/300 mA AC/DC power supply unit to the ZK-MasterIV from HW V 2.0 on. By this power supply unit one external reader at most may be powered via the RS285 B interface. Please note the information in figure 52.

### 3.2.2 Digital Input

Examples for use the digital Input of the MasterIV terminals.

☞

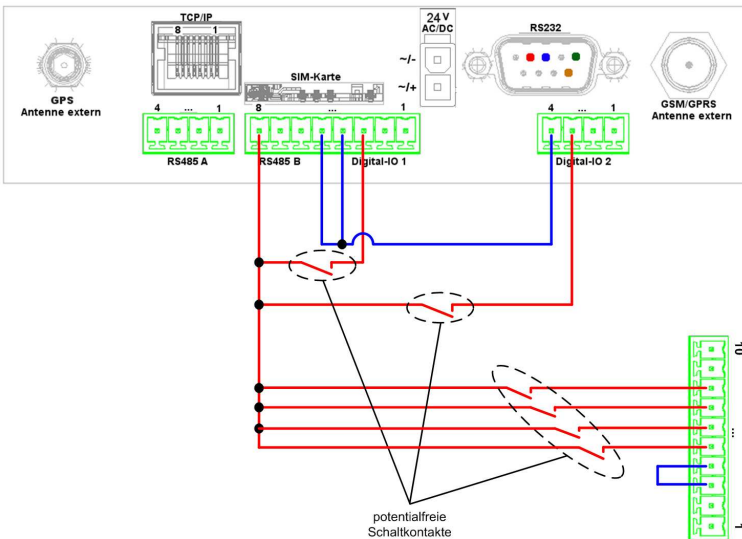
**Note:**

Please keep in mind, the 10-pole plug in the two figures below is not available by every device.

!

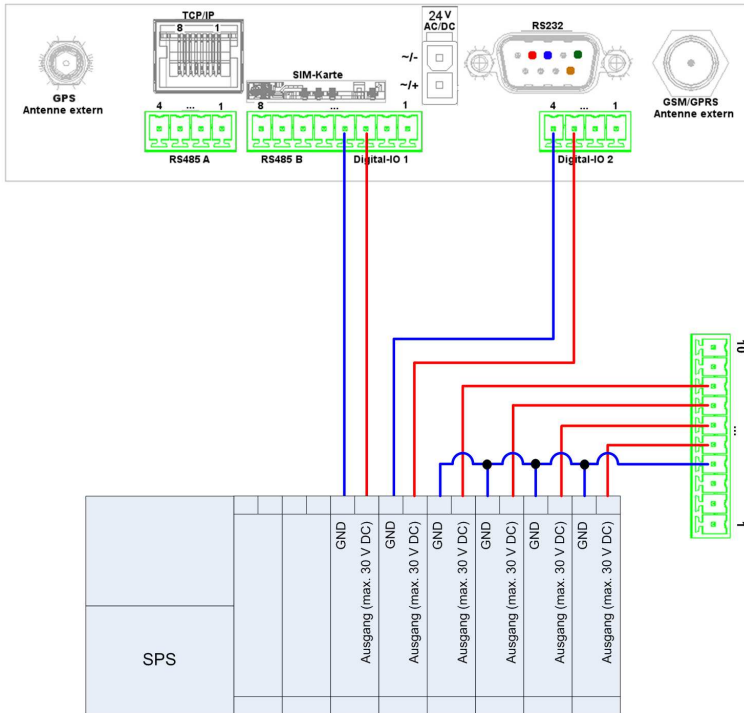
**Achtung:**

Note in any case to proper ones Signals.



This example displays the possibility for connection of potential-free contact to the digital input.

Figure 9: Digital-Input potential-free



This example displays the possibility for connection of a SPS with 24 V output (electricity of ca. 7 mA / port).

Figure 10: Digital-Input SPS

### 3.2.3 USB connector

The USB Type B connector (slave, **no** active USB controller) can optionally be led out of the device by a USB cable through the edge connector. By this, the ZK-MasterIV can be connected to a PC as USB terminal.

### 3.2.4 Ethernet interface

!

**Caution:**  
Power over Ethernet (PoE) describes a process with which network-compatible devices can be energised via the 8-core Ethernet-wire. The internal TCP/IP module of the ZK-MasterIV is not PoE tolerant.

The device can be integrated into a network of companies via TCP/IP via the RJ45 plug (2) in figure 7 and 8.

### 3.2.5 Mobile communications modem

At position (4) at figure 7 and 8 is the SIM card slot for an integrated mobile communications modem.

### 3.3 Commissioning

On delivery the device is already in working order and configured with a demo setup for a TS TMR33-LTM so that you immediately can test the access control. After having connected the door module via RS485 to the ZK-MasterIV (see chapter 3.6.2), you can establish the power supply by plugging in the power supply unit. The ZK-MasterIV automatically starts booting, recognition of the hardware options and loading the setups. Because the device has no display, you can only discern the booting by the flushing LEDs. After having finished booting the device automatically switches to the operating mode (8) in figure 7 and 8 is "ON" (9) is "OFF". Now the ZK-MasterIV is ready for use. Only use power supply units with appropriate power to establish the power supply (see chapter 3.2.1). Also note the information in figure 52.

On delivery the device is set for a communication via RS232 with 38400 Baud. Because the ZK-MasterIV has no display, changes that concern the device bios - which includes the change of the communication - can only be made via the DatafoxStudioIV. You can find further descriptions in chapter 4.5.12.

**Note:**

Before changing the communications read the corresponding paragraph in chapter 3.5.

### 3.4 Operation

#### General guidelines for the operation

Because the ZK-MasterIV has no display, all changes of the configuration of the device can only be made via a PC with the help of the DatafoxStudioIV. You can find a more detailed description in chapter 4.5.12.

### 3.5 Communications

The ZK-MasterIV has different interfaces for communication (dependent on features and hardware version). Thus, peripheral (e.g. bar code- or transponder reader) can be connected to the device or a communication with the device is possible. Because the device has no display, all configurations have to be made via the DatafoxStudioIV, see chapter 4.5.12. For this purpose the device has to be connected to a PC.

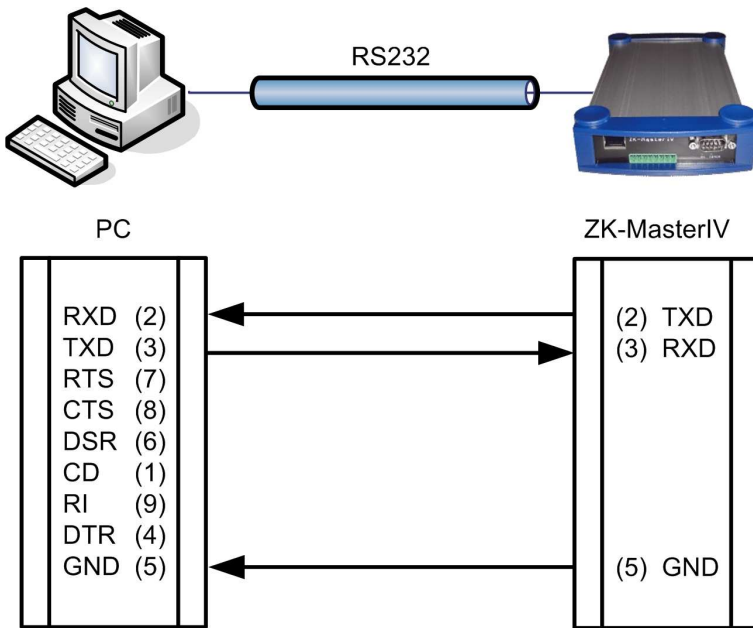
#### 3.5.1 Communication via RS232

##### 3.5.1.1 Requirement

For a communication with a ZK-MasterIV over an RS-232 connection, the device has to be set for this communication in the system menu-BIOS (see chapter 4.5.12). Furthermore, baud rate and timeout of the RS232-interface of the terminal and the PC must be coordinated. Permitted baud rates are 9600, 19200 and 38400. The timeouts have to be between  $\geq 100$  and  $\leq 2000$ . When you select RS232 for communication the timeout is set on 100 by default.

##### 3.5.1.2 Connection





A single device can be connected to the PC directly via the RS232-interface (position 1 in figure 7 and 8). The cable must not be longer than 15 m. Use a RS232 cable with a 1:1 configuration, corresponding to Datafox item no. 20010, as connecting cable.

Figure 11: Connection of the ZK-MasterIV with the PC about RS232

### 3.5.1.3 Conversion of RS232 to RS485

Up to 31 devices can be connected to a serial interface of a PC or server via a RS232-to-RS485 converter. In this case the devices are connected via a RS485 bus. The power supply can be established using a central power supply unit with adequate power. Note that the fall of voltage is dependent on wire cross-section and length.

The pin assignment of the converter will be demonstrated using the Datafox converter RS232/485 (small) as example. Gather the wiring of the RS485 bus from the following examples.

!

**Caution:**  
Pay attention to the hardware version given in the examples. It is a precondition for the prevailing example.

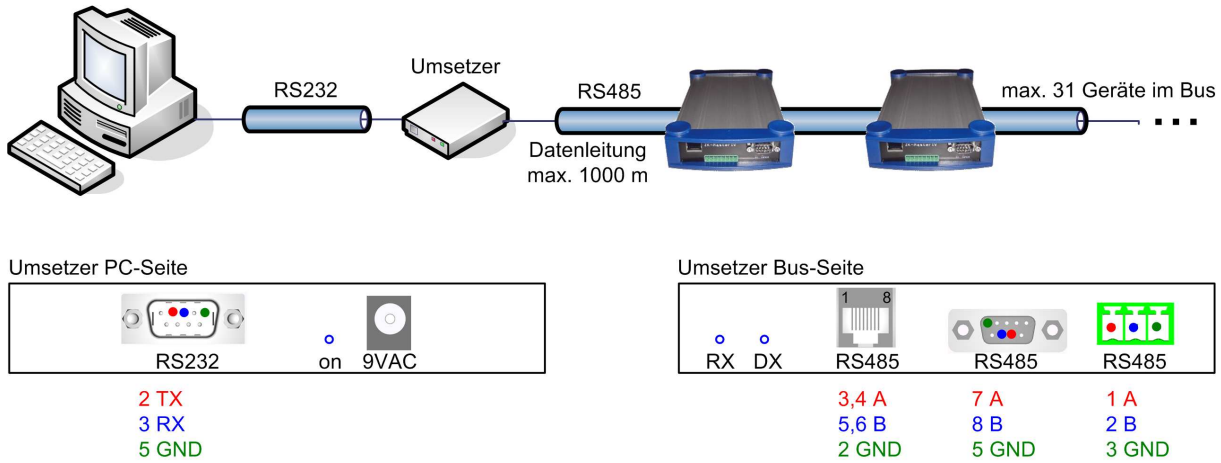


Figure 12: RS232 auf RS485 Bus

Connect the converter to the PC with a Sub-D 9-pole 1:1 cable as shown in figure 11. The converter replaces the ZK-MasterIV.

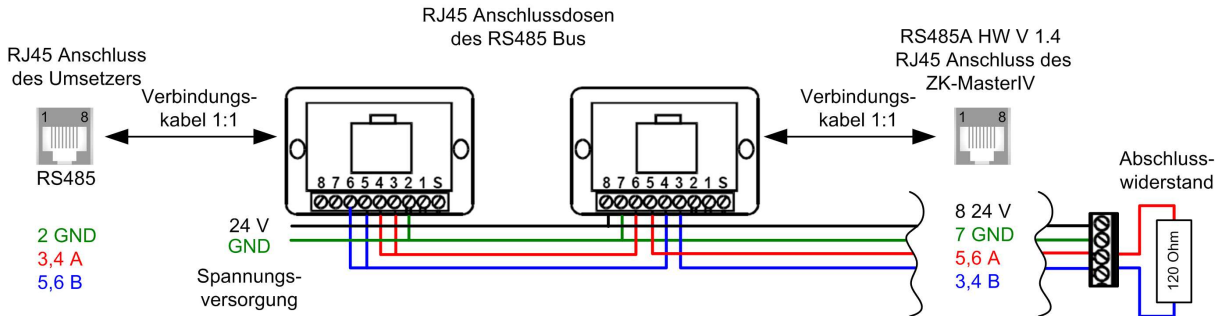


Figure 13: RS485 Bus über RJ45 (RS485A HW V 1.4)

PIN 3/4 and 5/6 are bridged in the device and makes it possible to loop the bus through. PIN 7/8 in figure 13 and PIN 1/4 in figure 14 are supply entries which make a power supply of the device via the bus possible.

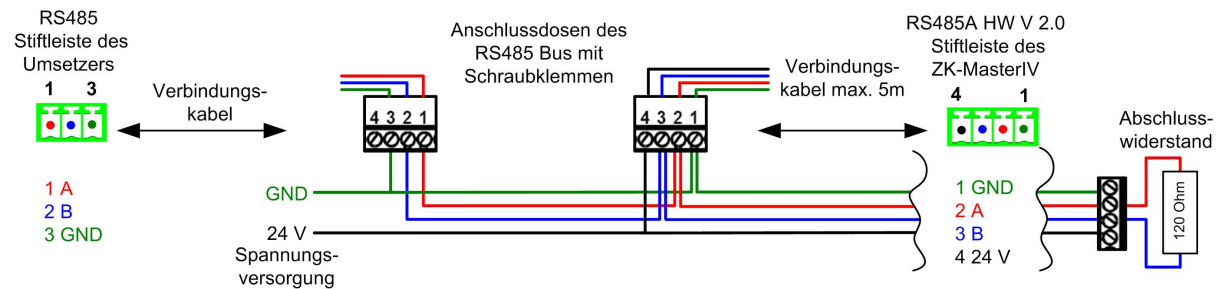


Figure 14: RS485 Bus über Stiftleisten (RS485A HW V 2.0)

!

**Caution:**

If the power supply of the ZK-MasterIV and the RS485 bus is established via PIN 7/8 (RJ45 connection of the ZK-MasterIV in figure 13) or PIN 1/4 (male connector of the in figure 14) direct voltage must be used (see chapter 3.2.1).

### 3.5.2 Communication via USB

**Note:**

Note that the USB-interface of the ZK-MasterIV is an USB type B. That means the ZK-MasterIV works in slave mode and therefore cannot manage other USB-devices.

#### 3.5.2.1 Conditions

You have to install the USB device drivers and the USB serial converter drivers that are necessary to communicate via USB.

**Caution:**

Only use the drivers provided with the device!

#### 3.5.2.2 Connection

The ZK-MasterIV is connected to the PC via a standard USB cable A-B.

#### 3.5.2.3 Driver installation

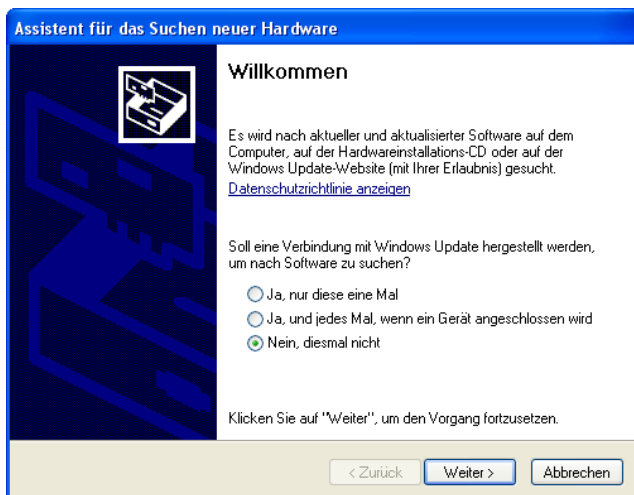
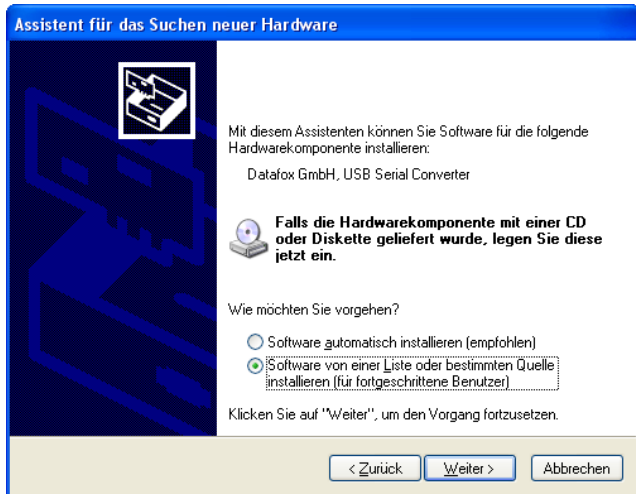


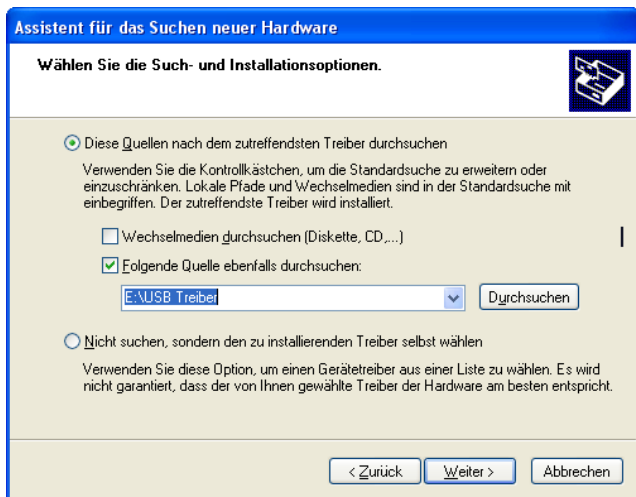
Figure 15: Automatic start of the setup assistant

After connecting the ZK-MasterIV to the PC, the terminal is recognized as new USB device and the installation of the provided USB drivers starts.



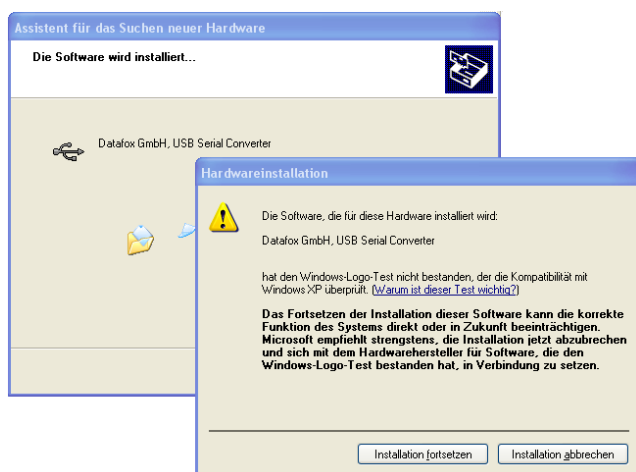
The next step is to set that you want to install the driver from a certain source.

Figure 16: Configuration of the setup assistant



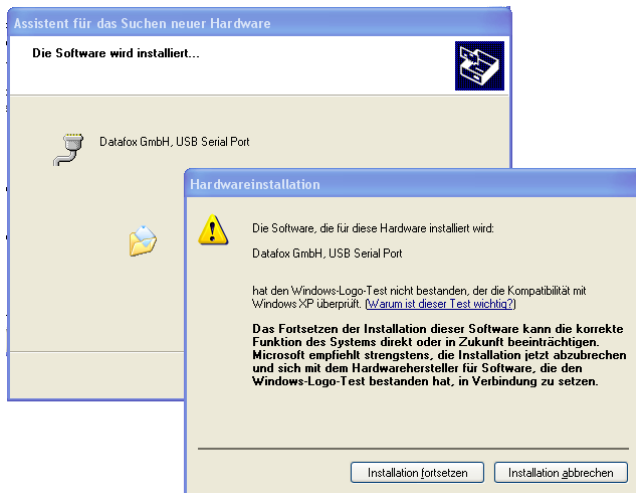
Select the folder of the driver file.

Figure 17: Selection of the source directory



Installation of the driver for the Datafox USB serial converter. The driver has no Microsoft logo, therefore the pictured message will be shown. Click on "Continue installation" to use the driver.

Figure 18: Datafox USB Converter



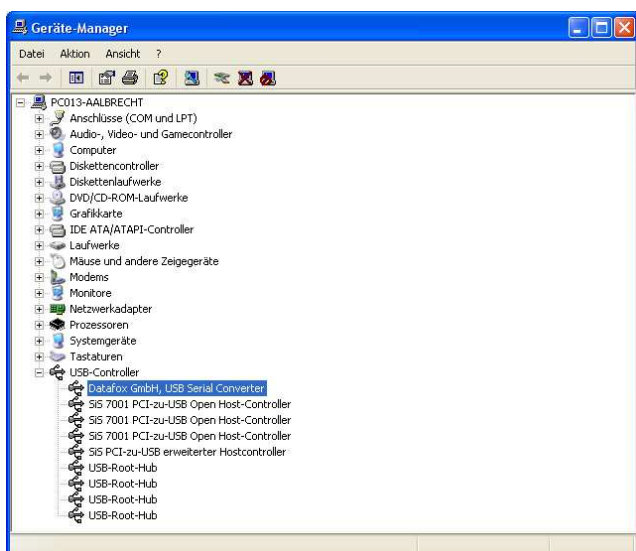
Driver installation for the virtual COM port. During this installation you will again get the message that the driver did not pass the Microsoft logo test. Click again on "Continue installation" to use the driver.

Figure 19: Virtual COM Port



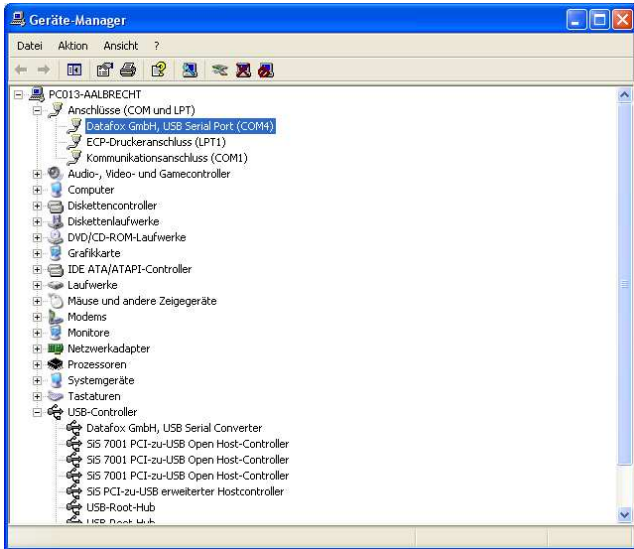
The driver installation is finished.

Figure 20: Driver installation finished



You can check the successful USB driver installation in the Device Manager. There have to be the following entries without a yellow exclamation mark.

Figure 21: Datafox USB Controller



The entry for the Datafox USB Serial Port is added as well. Via this COM-Port you can establish a connection to the ZK-MasterIV with the DatafoxStudioIV or with your own application via the DF-ComDLL.dll.

Figure 22: Datafox USB Serial Port

### 3.5.2.4 USB stick as data medium

In addition to the main communication USB, it is possible to use an USB stick as data medium. That way you can read out data records from a ZK-MasterIV and continue processing on a PC or create lists the for master data or the access control.

#### 3.5.2.4.1 Data structure and security

In order to guarantee the data transfer between the terminal and the USB stick, you have to create a directory structure on the USB stick at first. Please use the following application for this: USBMemoryStick.exe or DatafoxStudioIV.

Please plug an empty USB stick in the USB port of your PC before starting the program. Now start the application, mentioned above, and carry out the following steps.

In the steps 1 to 5 the data structure and the password are logged on the USB stick. With it all USB terminals are operated, irrespective of their serial number.

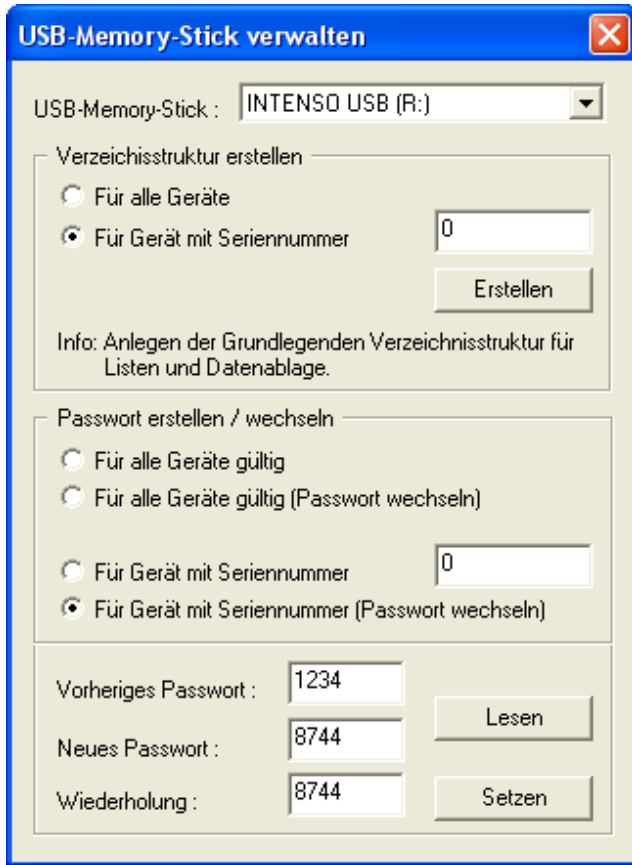


Figure 23: Configuration of an USB stick



Figure 24: File structure on the USB stick

The filing structure COMMON on the USB stick is used by all terminals, that support a main communication via USB. All \*.txt files, that are filed on the USB stick, have to correspond to the list descriptions in the setup (in designation\*, field size and format). Carry out a tabulator as field separator and CR + LF at the end of line.

\*The designations of the text files (lists or data) can only be selected in the format 8 dot 3. That means, that each text file has to be unique on the basis of its first 8 digits. If the list descriptions are not unique

1. Select the drive, that was allocated to the USB stick.
2. Create the directory structure for all devices, irrespective of their serial numbers.
3. Create a password, that is valid for all devices. The correct password is the basis of a data transfer between the terminal and the USB stick. Thus you avoid, that any USB stick with the created data structure can read the data out of the device.
4. Log the password, e.g. 1234.
5. Set the password to the USB.

A new directory structure COMMON, that is used as filing for the transfer data, was created on the USB stick.

Create the interface folder ACCESS for the access control lists, that are to be transmitted to the terminal. The lists have to be logged as \*.txt file. The folder DATA contains the data records (as \*.txt file), that were recorded from the terminal on the USB stick.

In the folder KEY the key (as \*.dat file) is logged, that allows a communication between the terminal and the USB stick. If no password was created, the file remains empty.

All lists (as \*.txt file), that are to be transmitted to the terminal, are filed in the LIST folder.

within the first 8 digits, a termination of the communication may occur. No lists are transmitted to the terminal then.

If you want to transmit data and lists terminal oriented, you have to log an additional data structure in the following steps. The selection is based on the serial number of the terminal.

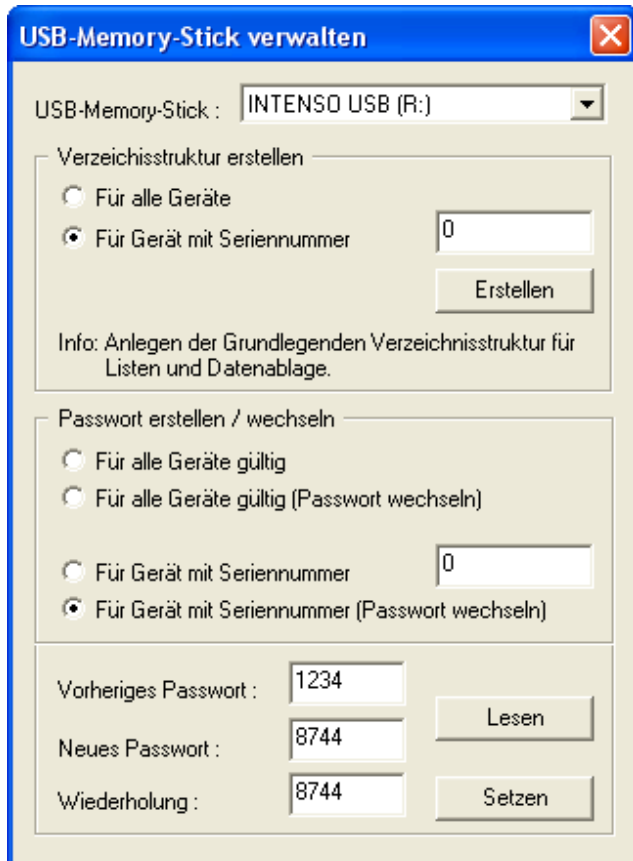


Figure 25: Configuration of an USB stick

6. Select the drive, that was allocated to the USB stick.

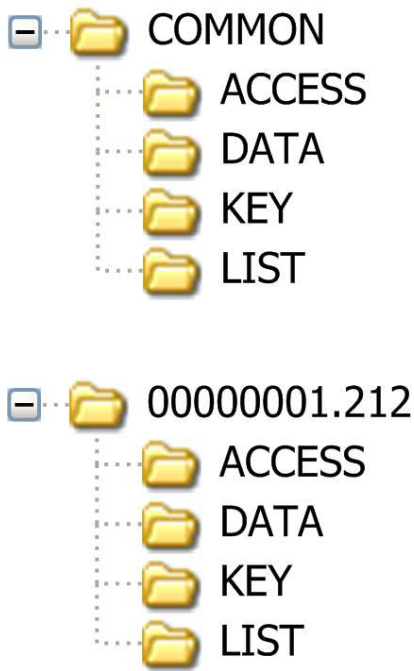
7. Create the directory structure for a terminal with the proper serial number.

8. Create a password, that is only valid for the terminal with the logged serial number (e.g. 1212). The correct password is the basis of a data transfer with this terminal. That way you avoid, that any USB stick with the created data structure can read the data out of the device.

9. Log the password, that shall be logged for this terminal only, e.g. 4455.

10. Set the password to the USB stick.





The already existing data structure (created in the first step) is used for all terminals, irrespective of the serial number.

Next, an additional directory structure only for the terminal with the serial number 1212 is created on the USB stick.

Interface folder for the access control lists, that are to be transmitted to the terminal (1212). The lists have to be logged as \*.txt file.

The data folder contains the data records (as \*.txt file), that are to be written from the terminal (1212) on the USB stick.

The key (as \*.dat file) is logged on the KEY folder. It allows the communication between the terminal (1212) and the USB stick. If no password was created, the folder remains empty.

All lists (as \*.txt file), that are to be transmitted to the terminal (1212), are logged on the list folder.

Figure 26: Filestruktur auf USB Stick

When communicating with the terminal (1212), the terminal only accesses to the directory structure created for that purpose. Thus, no transfer with the general directory COMMON takes place. An own directory structure can be created for each terminal.

When plugging the USB stick in the terminal for the first time, the setting and the logged password is recorded on the terminal. From this moment on, communicating is only possible, if the the correct password was entered.



**Caution:**

Note: This USB stick should only be used for the communication and the data transfer of terminal and PC. Data and folder structures, that are not related to the data transfer, might cause negative effects concerning the writing of data on the USB stick. A termination of communication with the USB stick may occur and data records may be damaged.

### 3.5.2.4.2 Change the password of the communication

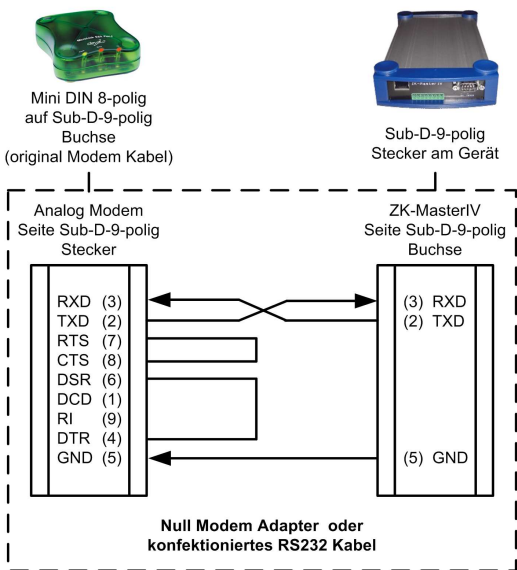
In order to change an already existing password on the USB stick and on the terminal, you have to use the same application, you already used for creating the directory structure.

### 3.5.3 Communication via analogous modem

#### 3.5.3.1 Conditions

For a communication via analogous modem, you have to set "RS232" as communication in the system menu-BIOS of the ZK-MasterIV (see chapter 4.5.12). The baud rate of the terminal and the connected modem must be coordinated. The timeout must be set dependent on the line quality of the telephone network (Which disturbance sources the cable is exposed to?). The worse the line quality the higher the timeout should be set. The modem to which the terminal is to be connected has to be configured via the COM-interface of a PC. The steps listed below refer to the tested and recommended "Devolvo-MicroLink 56k Fun II" modem.

#### 3.5.3.2 Connection

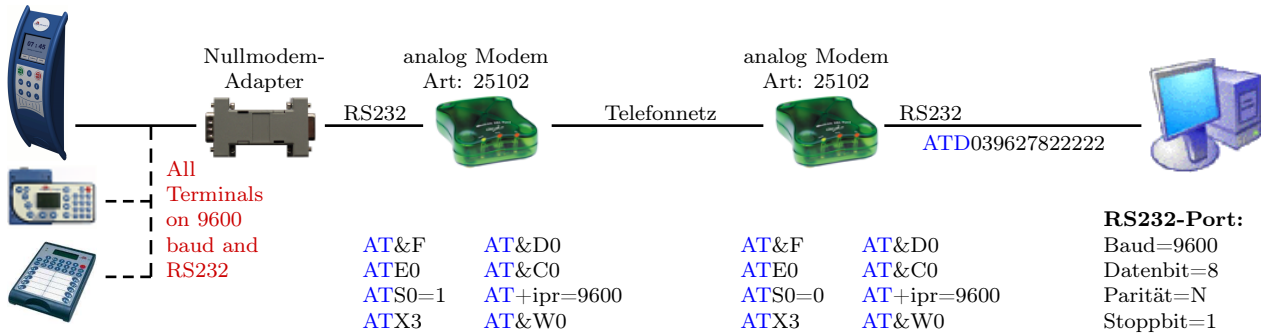


The analogous modem is connected to the COM-interface of the PZE-MasterIV. Use a Null-modem-adaptor or another cable that is assembled corresponding to the figure.

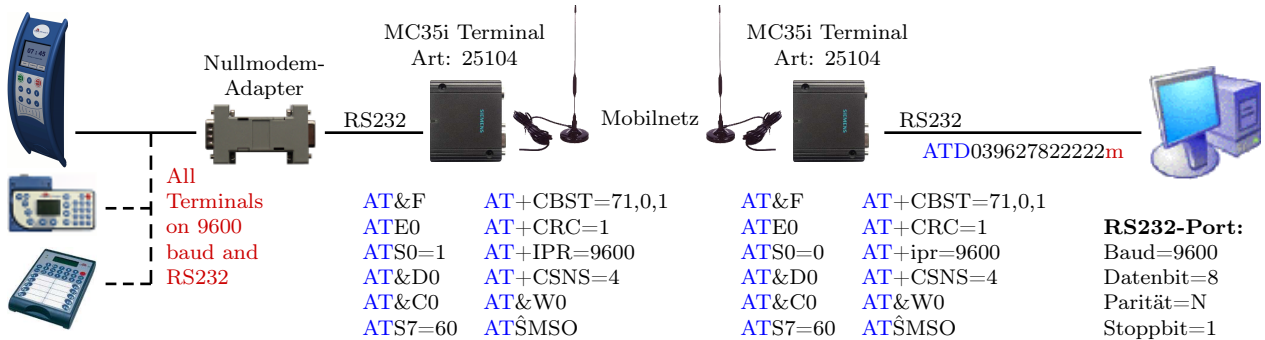
Note that at the site of the ZK-MasterIV **no** connections are bridged. You can use a Sub-D 9-pole 1:1 cable as an extension between the Null modem adaptor and the terminal.

Figure 27: Connection of the analogous modem to the ZK-MasterIV

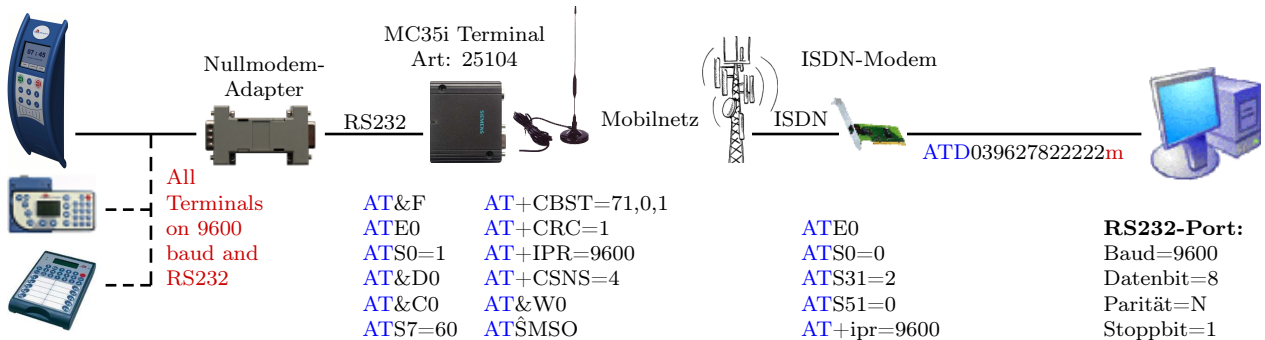
**Analogous modem to analogous modem** (Wiring of the Null modem adaptor see figure 28)



**Mobile communications modem to mobile communications modem** (Wiring of the Null modem adaptor see figure 28)



**ISDN (terrestrial network) to mobile communications modem** (Wiring of the Null modem adaptor see figure 28)



**ISDN (terrestrial network) to mobile communications modem (internal MC35i or MC55)**

All AE-IV Terminals with integrated GSM/GPRS-Modem



**Note:**

The configurations mentioned above are no guarantee for a connection. They are just based on experience and maybe have to be set to the different telephone systems. Configurations that are not listed here usually do not work.

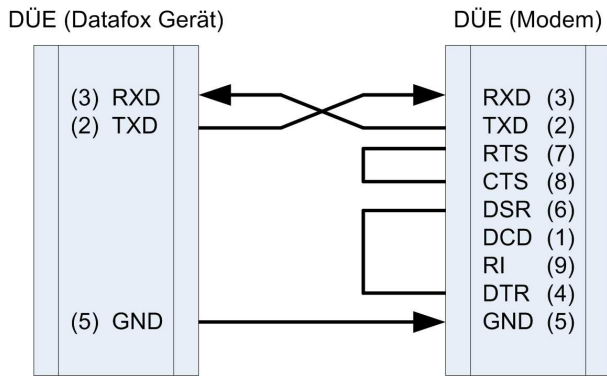


Figure 28: Wiring of the Null modem adaptor

Pin	Designation	Importance
1	DCD data carrier detect	Träger erkannt
2	RxD receive data	Empfangsdaten
3	TxD transmit data	Sendedaten
4	DTR data terminal ready	DEE empfangsbereit
5	GND ground	Signalmasse
6	DSR data set ready	Betriebsbereitschaft
7	RTS request to send	Sendeanforderung
8	CTS clear to send	Sendebereitschaft
9	RI ring indicator	Ankommender Ruf

Table 4: PIN Belegung und Kennzeichnung

Abbrevia- tion	Description
DCD	It becomes active when the connected modem has contacted another modem. It indicates the PC that a connection is established and data can be sent.
DTR	The computer signals his ready status, e.g. at a direct connection.
DSR	As response to DTR (at crossed lines.)
RTS	Becomes active when the terminal is ready to send data.
CTS	Becomes active when the terminal is ready to receive data.
RI	Is produced by a connected modem when a ring comes in.

Table 5: Description of the identifiers of the Sub-d-9-pole

**Output:**

Low-Pegel = + 12V

High-Pegel = - 12V

Output current: up to 10 mA

**Input:**

Low-Pegel is recognized till ca. + 1V

High-Pegel is recognized from ca. + 1V

Driving point impedance = 10 kOhm

### 3.5.3.3 Modem initialization

Check on which baud rate the ZK-MasterIV is set. You can find this information in the system menu-BIOS (see chapter 4.5.12).

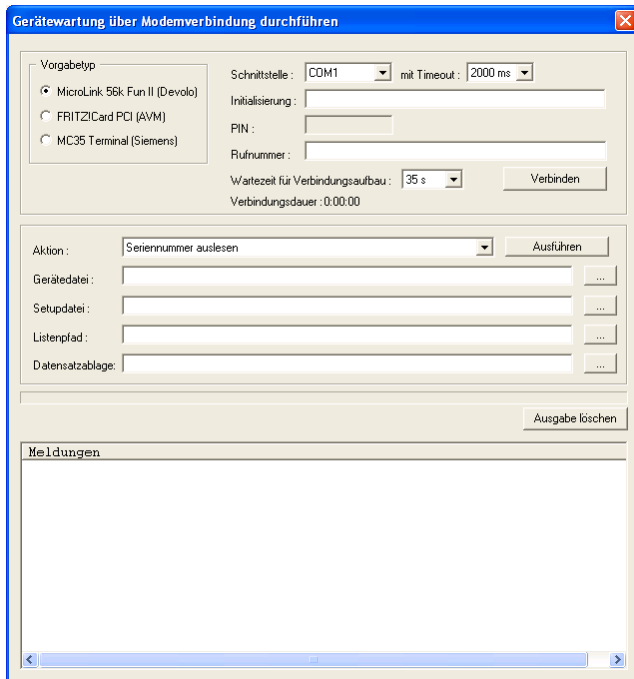


Figure 29: Configuration of the modem connection

Connect the "Devolo-MicroLink" to the COM-interface at your PC. Start the DatafoxStudioIV and open the modem configuration dialogue via *< setup => device maintenance via modem connection >*. Select "MicroLink 56k Fun II (Devolo)" as type and set a COM-interface of your PC out. Set the timeout on "2000 ms".

### 3.5.3.4 Connection via the DatafoxStudioIV

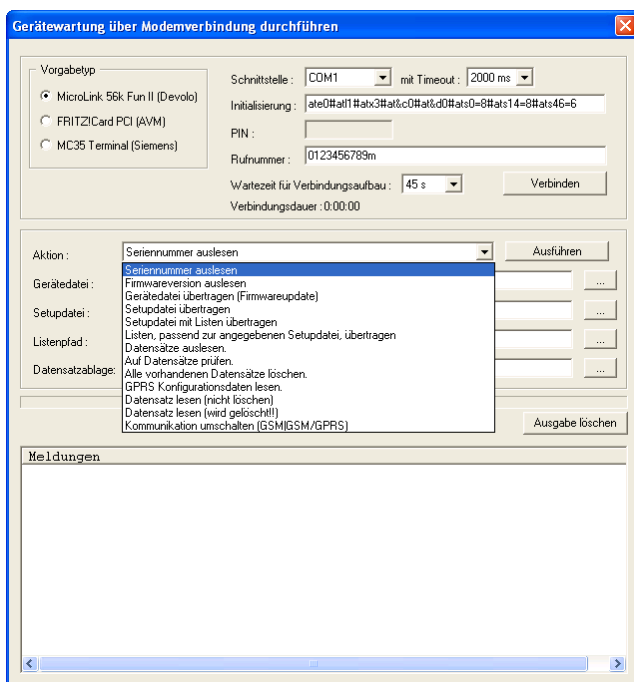


Figure 30: Dialogue for device maintenance via modem connection

Open the communication dialogue via the DatafoxStudioIV menu item *< setup – > device maintenance via modem connection >* to establish a connection between a ZK-MasterIV and a PC (DatafoxStudioIV). In dependence on the selected modem type you additionally have to set the COM-interface, baud rate, PIN and phone number of the remote station. Parameters that are not needed are deactivated.

This kind of communication is used at the administration of the ZK-MasterIV ("device maintenance via modem connection"). For this purpose different functions are available.

You can find further descriptions in chapter 4.4.5.

### 3.5.3.5 Connection via the DFComDLL

You can also start the connection to the ZK-MasterIV from your own application. Use the functions of the DFComDLL.dll to establish a connection between a PC and the device. Proceed as it is shown in the figure below.

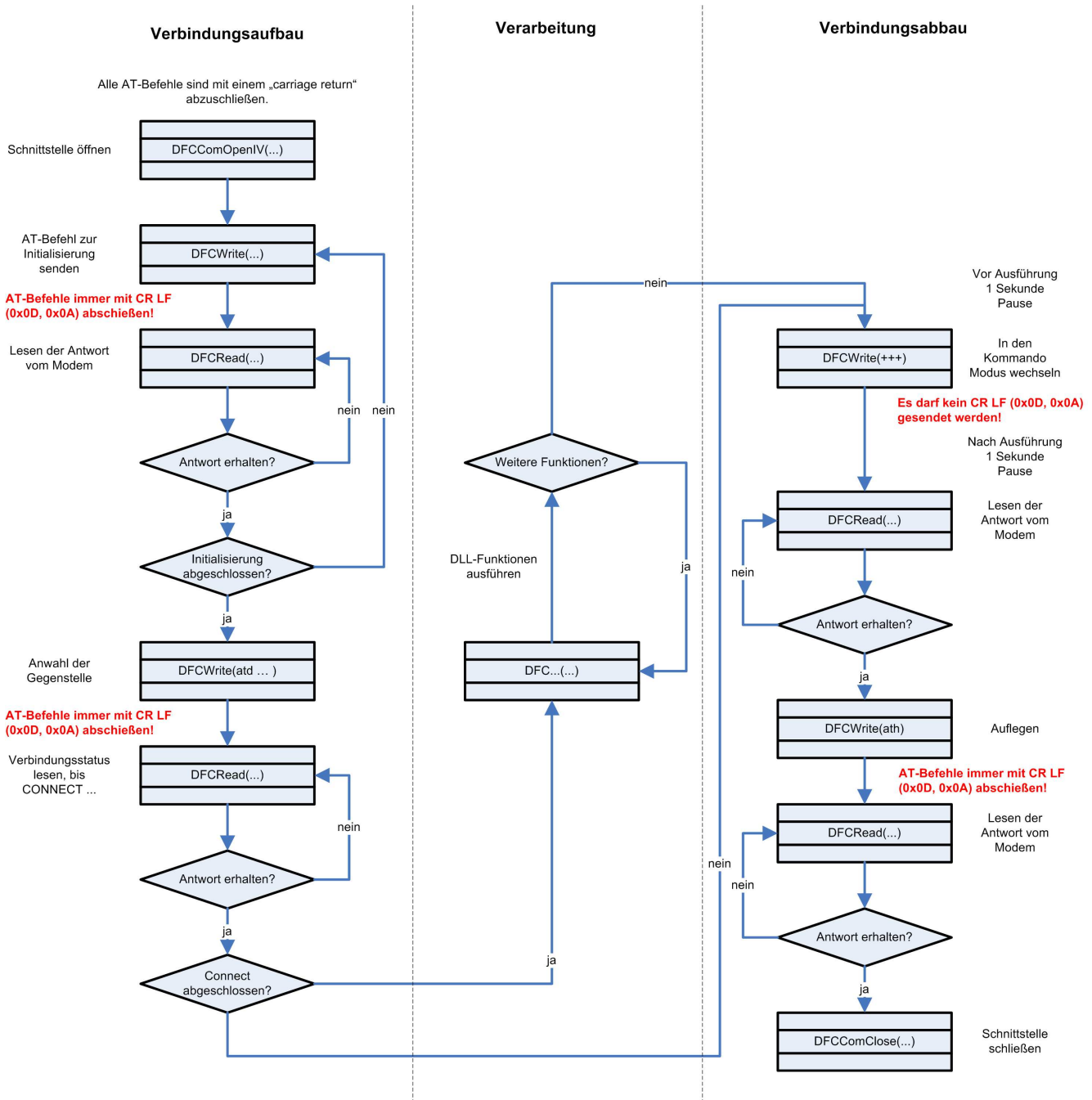


Figure 31: Course of the communication via DFComDLL.dll

You can find a more detailed description of the functions and parameters in the documentation or help to the DFComDLL.dll.

### 3.5.4 Communication via GSM or GPRS/GSM

The ZK-MasterIV can optionally be equipped with a mobile communications module (Siemens MC35i, MC39 or MC55) for GSM and GPRS to use it at locations without fixed or DSL network.



**Caution:**

GSM and GPRS are services that generate costs. Contact your provider to get further information about tariffs and generated costs.

Via GSM all functions of the DLL can be used. Currently, GPRS is used only to send data from the ZK-MasterIV to a web server. The advantage is that the data is sent immediately.

#### 3.5.4.1 Preparation

Put the SIM-card in the ZK-MasterIV before bringing the device into service. An external aerial has possibly to be connected; this depends on the selected hardware option (internal or external aerial). See chapter 3.2.5. In the BIOS of the ZK-MasterIV "GSM" or "GPRS/GSM" has to be activated as interface (see chapter 4.5.12).

#### 3.5.4.2 Configuration



**Caution:**

Starting from version 04.01.06 the internal TCP/IP stack of the modem is used. An existing GPRS radio connection is cut when no data is send for a period of 20 seconds after the last HTTP communication. With the next data the modem dials in again. This can cause higher communication costs, especially with low volume rates. This timeout is increased from 20 seconds to 8 hours from version 04.01.06.16.

You have to create a configuration file with the access data of your provider and transmit it to the device to use "GPRS/GSM". See chapter 4.5.11 for further descriptions of the parameters, the creation and the transmission to the device.



**Note:**

Note that the GPRS configuration files can be transmitted to the device only with the DatafoxStudioIV via RS232 or TCP/IP.

A communication via GPRS requires "GSM", therefore a SIM-card has to be put in the device (see chapter 3.2.5). For the SIM-card activation in the ZK-MasterIV the following scenarios are possible:

- 1.) You want to switch from another communication to a communication via "GSM" or "GSM/GPRS". Remove the device from the power supply and display the SIM-card. Go to the bios modus via the DatafoxStudioIV and set the interface at "GSM" or "GSM/GPRS". Transmit the changed bios configuration to the terminal and leave the bios modus.
- 2.) You want to switch from another communication to a communication via "GSM" or "GSM/GPRS". Remove the device from the power supply and display the SIM-card. Go to the bios modus via the

DatafoxStudioIV and set the interface at "GSM" or "GSM/GPRS". Transmit the changed bios configuration to the terminal and leave the bios modus.



**Caution:**

If a wrong PIN was transmitted to the device three times, the PUK has to be entered together with the PIN to activate the SIM.

**3.5.4.3 Connection state**

After transmitting the .ini'-file to the device the operating mode of the ZK-MasterIV can be set to "GSM/GPRS", see chapter 4.5.12.

GSM: The communication takes place via GSM.

GPRS/GSM: The data records created in the device are sent immediately to a corresponding web server via GPRS. All other functions have to be carried out via GSM.

The GSM state is shown via the state LEDs at the ZK-MasterIV (valid from version 04.01.01.21 on):

ERROR	POWER	GSM/GPRS	State of the device
On	On	Off	Bootloader
On	On	On	Start
Off	1 Hz	Off	Booten
1 Hz	1 Hz	-	No setup
1 Hz	On	-	Stopping of control mode
Off	On	-	Normal operation
Off	&	-	Communication active
Off	-	Off	Mobile, offline, not in the net
Off	-	*—	Mobile, offline, enrolled in the net
Off	-	On	Mobile, online
2 Hz	-	*—	Mobile, no SIM-card
2 Hz	-	**—	Mobile, PIN is required
2 Hz	-	***—	Mobile, PUK is required
2 Hz	-	*~	Mobile, other errors

Legende

-	LED - condition undefined
Off	LED off
On	LED on
1 Hz	LED flushes once per second
2 Hz	LED flushes twice per second
&	LED turns off for about 30 ms
*	LED turns on for about 150 ms
~	LED turns off for about 150 ms
—	LED turns off for about 1000 ms
—	LED turns off for about 2500 ms



### 3.5.4.4 Send data via GPRS

The ZK-MasterIV can send booking data promptly to a web server via GPRS. For this it is necessary to configure the device for this communication as described above. When data is created in the ZK-MasterIV, firstly a TCP/IP connection is established and then the following character string is sent:



#### Caution:

Currently, no blanks or umlauts can be transmitted via GPRS. This problem is known and dealt with.

GET example/getdata.php?table=datensatz&parameter1=wert1&parameter2=wert2&checksum=pruefsumme

- ▶ GETexample/getdata.php? is the prefix of the HTTP data and gives the path on the web-server where the php-script is with which the HTTP data are processed.
- ▶ Table is a data record description from the setup (the table from which data are to be transmitted).
- ▶ Parameter *n* describes the field names from the data record description (table field).
- ▶ Checksum is to detect errors at the data transmission

You should enter only a few characters for the tables and field names to have a small transmission volume.

The checksum is the sum of all ASCII values of the transmitted parameter values (only of the values, not of the filed name; that means everything that is written between = and &). The web-server has to send back the following answer within HTTPTIMEOUT:

- 1.) Success (checksum correct): status=ok&checksum=pruefsumme Then the data record is deleted in the ZK-MasterIV.
- 2.) Error (checksum incorrect): status=error&checksum=pruefsumme Then the last data record is sent again.



#### Caution:

Every answer string from the server has to end with 0x0D 0x0A.

As fixed parameters it has to be given:

"status=ok&checksum=" or "status=error&checksum="

The following optional parameters are allowed:

"&time=" the timestamp of the server is passed

"&message=" a message is passed to display it

"&delay=" sets how long a message is displayed

"&beep=" sets the kind of signal 0 = none, 1 = 1 x long, 2 = 2 x long,

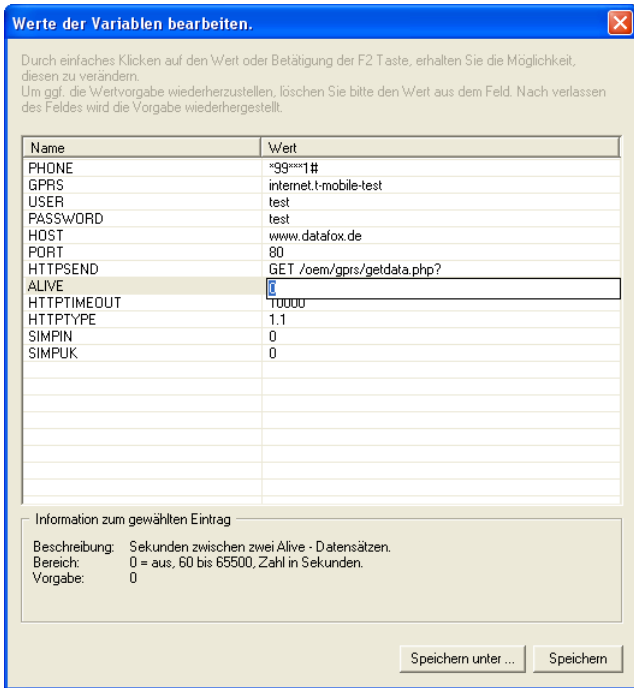
3 = 1 x short, 4 = 2 x short and 5 = 3 x short

If you want to adjust date and time of the ZK-MasterIV and the server, you can do it in the answer to the ZK-MasterIV as in the following example:

status=ok&checksum=3142&time=2003-10-28\_17:00:55

Now the ZK-MasterIV sets its internal clock on 17:00:55 and the date on 28 Oct 2003.

If connection problems occur, the error analysis can be simplified with the help of an alive-data record. Via the alive- data record you can detect if the device was on- or off-line, e.g. at the moment of power outage. You also can detect if the web-server was reachable all the time with the aid of the alive-counter in the alive-data record. With each failed attempt to send data the alive-counter increases. If no data reach the server and the alive-counter in the alive-data record has the value 1, the device has been removed from the power supply.



Activation of the function Alive via the parameter "Alive" (cycle for the creation of the alive-data record in seconds) with a value higher than 60 and lower than 65500.

The data fields of the alive-data record you should define in any case are the device number, date and time and the alive-counter.

The value of the alive-counter \* cycle for the creation = duration of interference. With this formula you can calculate the duration of interference via the alive-counter.

Figure 32: Activation of the alive-data record

**Note:** After three failed attempts to send data, the ZK-MasterIV starts the device regeneration with a timeout of 15 minutes. When the timeout is run out three attempts to send the data are started again. Thus, the generation of unnecessary costs is prevented.

**Caution:** Alive data are temporary data. If the alive-data record cannot be sent (e.g. server is nor reachable), it will be deleted and the alive-counter will be increased by one. The function "alive" is activated via the alive parameter in the GPRS.ini. Additionally to the activation the F6-chain or (from version 04.01.04.x on) or the GPRS-chain has to be available in the signal processing. Take care that this function does not create unintentional data (traffic).

### 3.5.5 Communication via TCP/IP

Usually, the configuration of the network connection is necessary to integrate a ZK-MasterIV. But if a DHCP server, that supplies all PCs and peripheral with dynamic IPs, is available in the network, this configuration can be omitted. In this case the IP of the terminal has to be set on "000.000.000.000".

- ▶ **version** fixed value
- ▶ **MAC** fixed value
- ▶ **IP** changeable value
- ▶ **port** changeable value, analogous IP
- ▶ **hostbits** changeable value, analogous IP
- ▶ **gateway** changeable value, analogous IP
- ▶ **remoteaccess** changeable value you have the choice between **yes** and **no**.
- ▶ **set default** the default values of the device are set

A possible access protection per Telnet or web interface to the TCP/IP module of the Datafox terminal is deactivated after a restart of the device.

Starting from version 04.01.06.16 the following security mechanisms are available:

Variant 1 A complete protection of the terminal against remote access (Telnet-session, web interface) is possible by deactivating remote access in the BIOS of the device. Then TCP/IP settings are only available at the terminal itself.

The settings for the remote access (yes / no) in the BIOS can only be changed if the BIOS is protected by a password. This means that after a firmware update it is necessary to transfer a setup with a BIOS password before the settings can be changed.

This additional protection is necessary because a change of this setting (remote access yes/no) deactivates a probably set Telnet password.

Variant 2 In a Telnet session you must set the value for "Enable Enhanced Password" to y (yes) in menu 6. Also set the value for "Change the password" to y (yes) and enter the password. Save these changes at menu item 9, Save and Exit. With these settings you have protected the access per Telnet as well as per web interface with a single password. With this variant you can still change the settings per remote access.



**Caution:**

Important! A change of the setting remote access in the BIOS of the device deactivates the Telnet Enhanced password. This can be desired if you forget the password and want to reset the terminal. To do so you need the BIOS password which can be found in the devices setup.

A firmware update has no influence on the security settings of the terminal!

### 3.5.5.1 LAN

Analogous to the direct connection via RS232 a single device can be connected directly to the PC via TCP/IP. In this case the device is connected to the PC with a CAT-5 network cable (in case of direct connection with crossover; in case of connection via router,... with patch cable) via the RJ45 jack. Please note that the RJ45 jack can also be the RS485 port at "HW V 1.4" (see figure 7 point 2). The device must have the option TCP/IP.

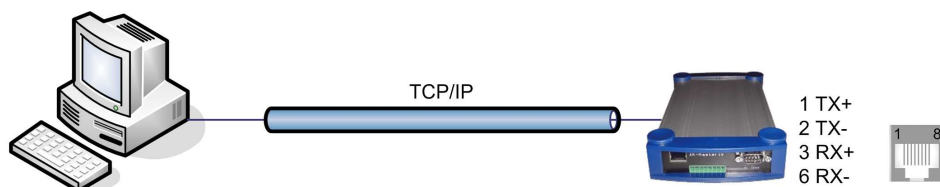


Figure 33: Connection to the PC via TCP/IP

### 3.5.5.2 Transition from TCP/IP to RS232

In order to connect a single device via RS232 to a TCP/IP network a COM-server has to be used. The COM-server serves as converter.

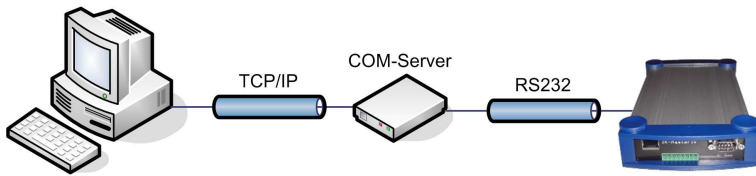


Figure 34: TCP/IP to RS232

The necessary settings of the COM-server will be explained using the W&T COM-server as example. The COM-server can be configured easily via the Wutility.exe program.

- 1.) Open the W&T program
- 2.) Open "inventory" and then "scan local network"
- 3.) Mac-address is displayed at the menu; click on it
- 4.) Adjust IP-address via "Configuration" and "Assign IP-Address"
- 5.) Click on telnet (screen) button
- 6.) The telnet menu is shown
- 7.) Press key 3 (setup port 0) and then 2 (UART setup)
- 8.) Further settings see below
- 9.) Save setup and close program
- 10.) Hardware settings see manual of the COM-server

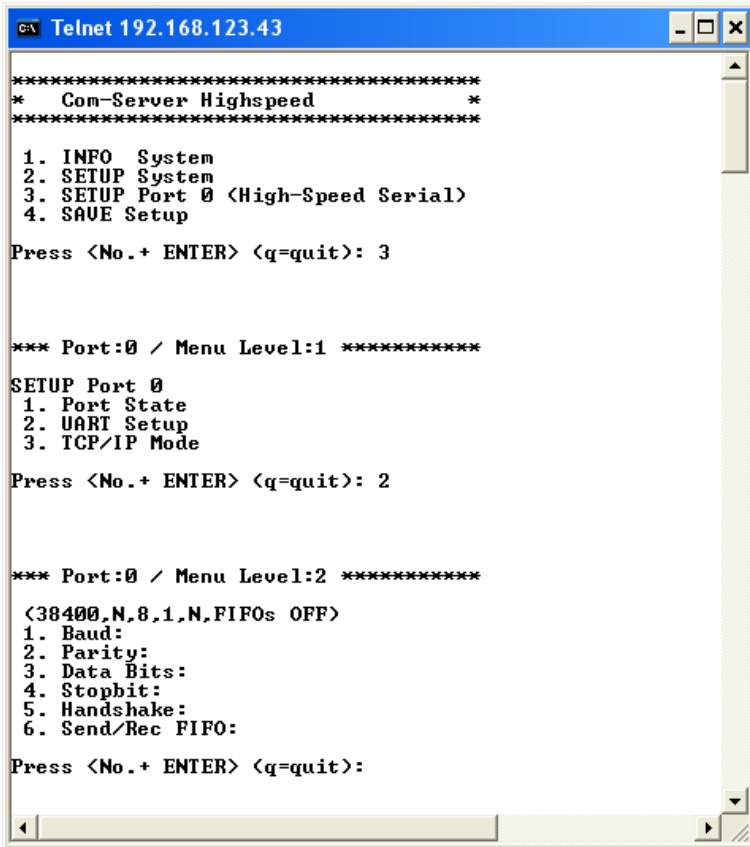


Figure 35: COM-Server configuration over telnet

### 3.5.5.3 Transition from TCP/IP to RS485 Bus

Up to 31 devices can be connected economically via a COM-server with RS485 bus. You can find details about the structure of a RS485-network in the separate networking description. You can request it from us or download it from our homepage. Please note that the bus number has to be set directly at the terminal (see chapter 4.5.12).

The network structure is a bus. The bus cable is looped through from one device to the other. Branching is not allowed. The PC can be connected at the beginning, the end or somewhere in the middle of the network. The total length of the bus cable must not exceed 1000 m.

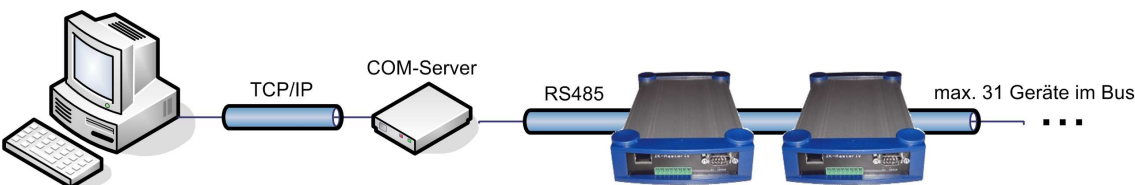


Figure 36: TCP/IP to RS485 Bus

### 3.5.5.4 WLAN

The ZK-MasterIV can be integrated into a WLAN with a WLAN router via TCP/IP. Please note that a WLAN router is an external component and that you have to pay attention to the compatibility to the present network topology. You have to set the IP-addresses in the system menu bios of the ZK-MasterIV and the WLAN router in accordance with the network class of the present network.

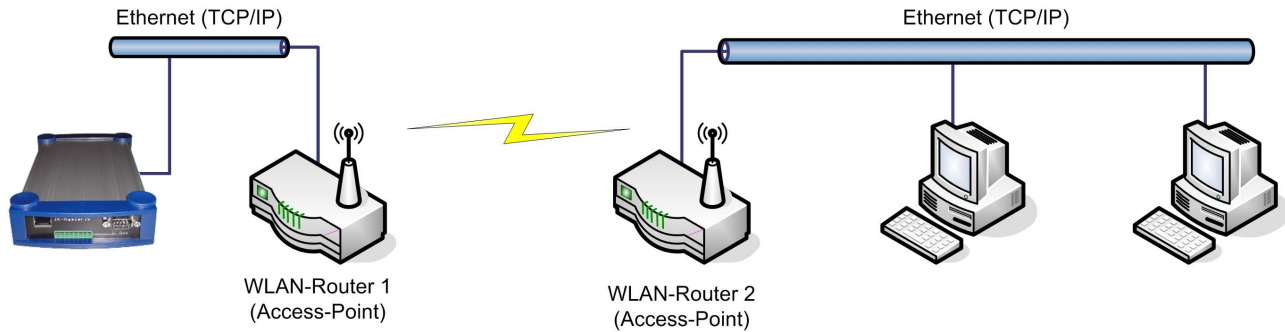


Figure 37: Connection of a ZK-MasterIV via WLAN router to a WLAN network of a company

### 3.5.6 Communication via RS485

The RS4485 Datafox Network is based on Modbus. Modbus is a simple and safe bus system and is also used in measurement technology.

RS485 is no standard communication of PCs, therefore you need a converter to set up this kind of network. See chapter 3.5.1.3 for the connection and the wiring for a transition from RS232 (PC) to a RS485 net and see chapter 3.5.5.3 for the transition from TCP/IP (PC) to a RS485 net.



**Caution:**

It is possible that the RS485 interface is available in the form of a RJ45 jack at devices of HW V 1.4 . Check if the RJ45 jack is a RS485 interface before you connect an external voltage source to PIN 7 = GND and 8 = 24 V DC.



**Note:**

All components for the RS485 - interlinking can be ordered with the devices. You find the articles in the suitable price-lists or on inquiry.

The bus line connects the converter and 31 ZK-MasterIV at most in series. Branching is not allowed. The converter can be connected to the bus line at any place. The maximum total length of a bus cable is 1000 m. The bus line should be laid in trunkings at the ceiling or the wall. In order to connect a ZK-MasterIV the data line is wired to a Cat. 5 outlet and connected via a RJ45 patch cable or via outlets with terminal strips via a stub line from the RS485 bus to the terminals. You can connect one Datafox-Bus per RS232 interface at the PC. You can install as many busses as you like also at different PCs. One communication program per bus is active to operate the communication between the single devices and the central data server. Because of potential differences a Datafox-Bus line should not be laid between different buildings. This connection should be mainly realized via the PC network via glass fibre.

### 3.5.7 Active connection via TCP/IP

An active connection is supported from the firmware version 04.01.05.x on. This function is available for the main communication TCP/IP, WLAN and GPRS (only from the GSM-module MC55 on)

The connection is always bidirectional full-Duplex. The communication is based on the Datafox protocol of the MasterIV series.

#### 3.5.7.1 Description

The concept for an active connection contains the realisation of an initialisation of the TCP/IP connection between the device-software (firmware) and the DLL-software. The connection is always initialized by the firmware. The link negotiation is done via appropriate commands with the DLL.



**Note:**

Note: For most providers a TCP/IP connection establishment "from the outside" is not possible. Therefore the connection has to be established by the firmware. Either the connection requests are blocked directly by the provider or the IP-address established by the PC is not the real one of the device.

A connection establishment can be done in TCP/IP networks (also GPRS). The devices do not permit several connections at the same time. Therefore no other connections must be established in order to initialize the connection establishment.

In principle, a connection request of a Device to the DFComDLL is processed as follows:

The DLL receives a connection request on a listen socket. The connection administration checks, whether a port object can be created. After creating a port object, the connection is established and remains for further applications.



### 3.5.7.2 Configuration of an active connection

An active connection requires that the following parameters are set or configured in the ZK-MasterIV or the application (DFComDLL.dll):

- ▶ **com.active** (0 = deaktiviert, 1 = aktiviert) Switching on/off the active connection.
- ▶ **com.notify** (0 = deaktiviert, 1 = aktiviert) Switching on/off the active data record message.
- ▶ **com.prio** (0 = höchste, 65535 = niedrigste) Priority of the event messages in the queue.
- ▶ **com.host** (0.0.0.0 bedeutet alle) Host to one connection should be produced.
- ▶ **com.port** Port to one connection should be produced.
- ▶ **com.retry** Number of the attempts for connection setup.
- ▶ **com.timeout** Time out, after the set number has failed because of connection setup attempts.
- ▶ **com.repeat** The time out if by successful message about present records these were not retrieved, until a renewed message should be carried out.
- ▶ **com.alive** Time out, when the terminal diminishes an existing communication channel (connection quit) if no Kommunikation takes place. The DLL must send, if a communication channel should not be diminished, cyclically a Ping to the ZK-MasterIV.
- ▶ The bus address of the DLL (for call of DFComOpenIV) is firmly given with 31. The number of at the same time existing connections is delimited per DLL instance to 50 connections.

Here you have to pay attention to the following value margins and default values:

Description	Name of the system variable	Range of values	Default value
Activation	com.active	[0..1]	0
Active data record message	com.notify	[0..1]	1
Priority	com.prio	[0..65535]	0
Host	com.host	[IP-Adresse]	0.0.0.0
Port	com.port	[0..65535]	8000
Connection	com.retry	[0..65535]	3
Communication timeout	com.timeout	[0..4294967295]	900
Notification retry	com.repeat	[0..4294967295]	60
Connection check	com.alive	[0..4294967295]	0

Table 6: Parameters and default values for the configuration of an active connection

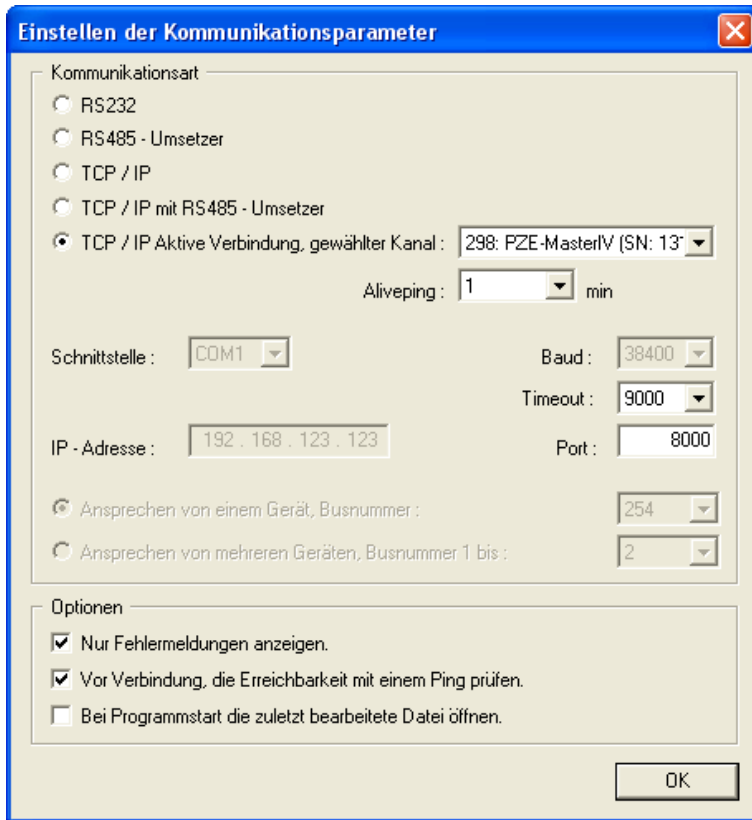


Figure 38: Active connection configuration

The parameters can be changed via the dialogue active connection configuration in the communication menu and be transmitted to the ZK-MasterIV. You may find information about the single parameters in the table 6.

Grafik muss noch angepasst werden

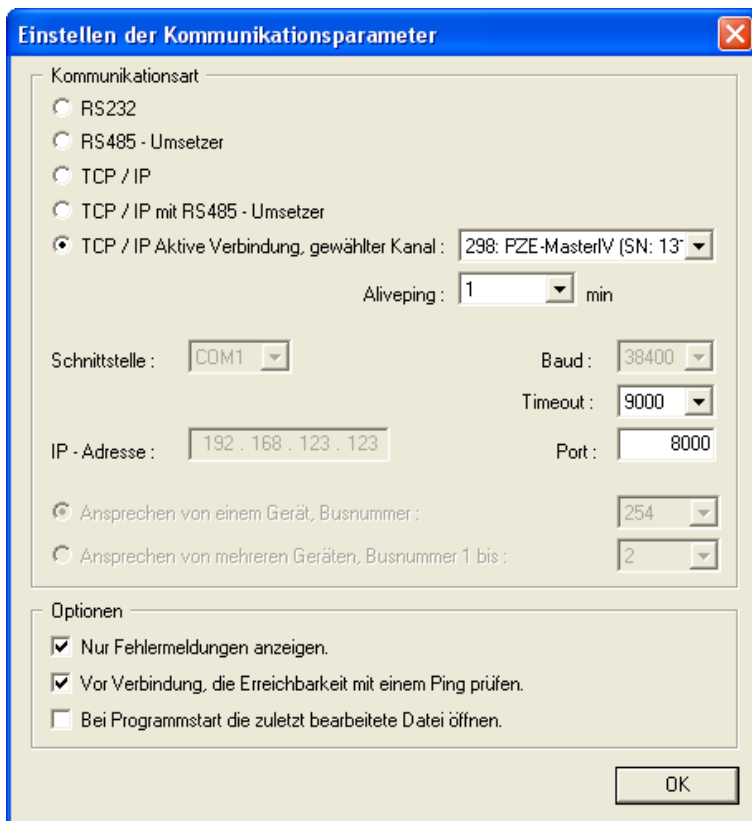


Figure 39: Setting the communication via the ZK-MasterIV

The configuration of a ZK-MasterIV via the DatafoxStudioIV with an active connection requires an active communication port (selected port: see figure on the left) from the device to the DLL. Set the alive ping, the communication timeout and the port according to your demands on the configuration. Afterwards all functions of the DatafoxStudioIV can be used in order to configure the device.

### 3.5.7.3 Device servicing via active connection

The following overview shows you the single procedures of the active connection and the possibilities for the servicing of the terminals.

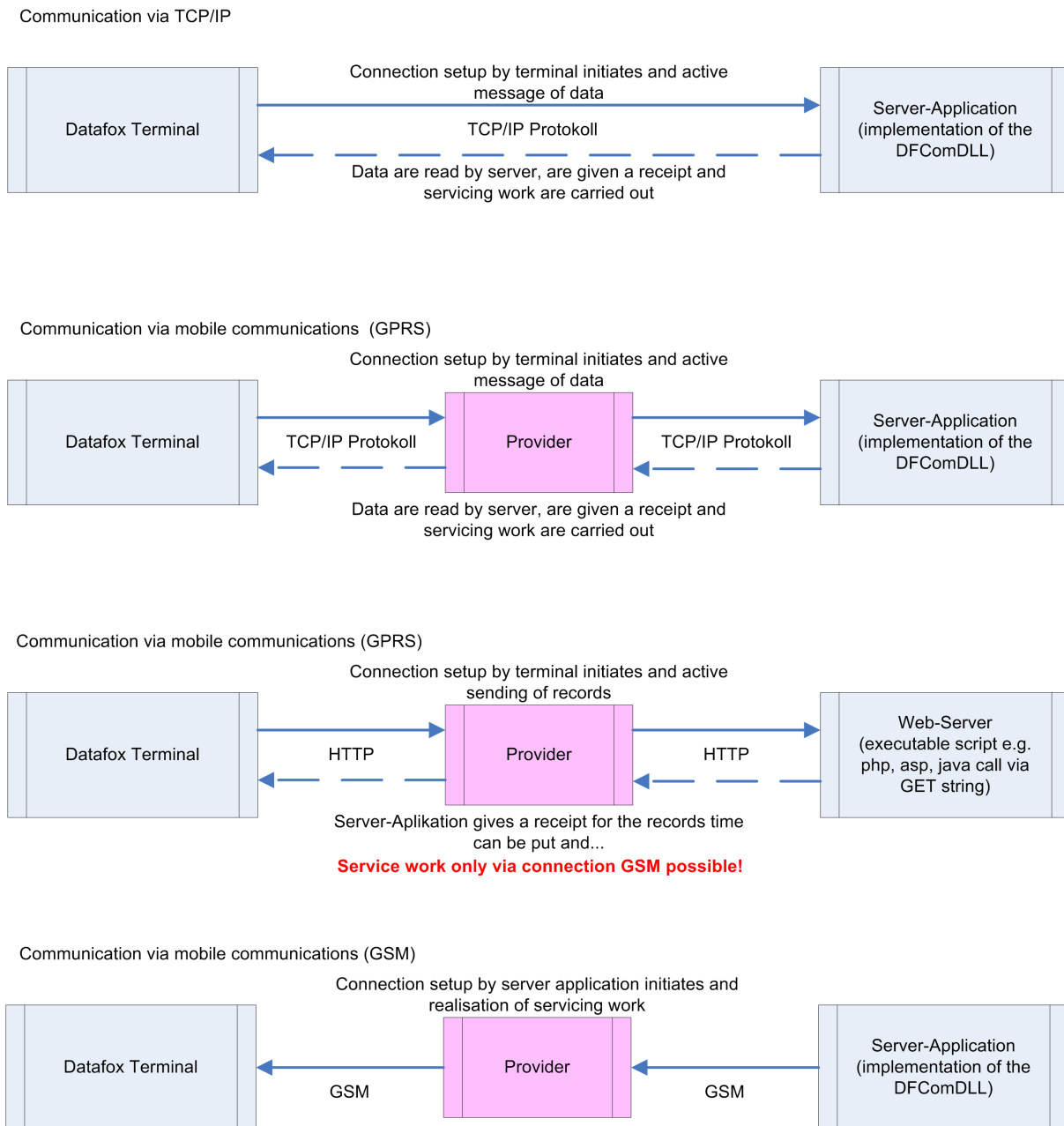
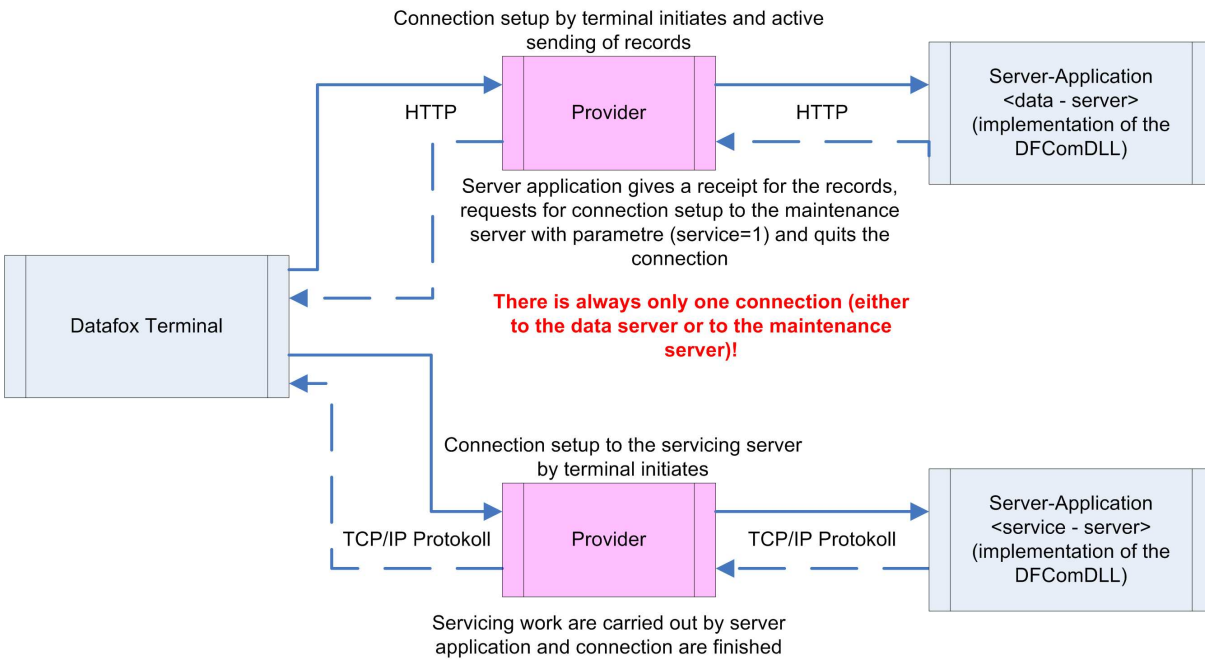


Figure 40:

Communication via mobile communications (GPRS)



### 3.5.8 WLAN

#### 3.5.8.1 General information

There are two possibilities to configure the match port. Either via the TCP/IP with the DeviceInstaller™ of Lantronix® or via the RS232 using the tool WLANConfig and the DatafoxStudio (from version 04.01.06.xx on).

#### 3.5.8.2 Terms and explanations

##### 3.5.8.2.1 Infrastructure Mode

(Loose translation of an excerpt from the German version Wikipedia, the free encyclopaedia)

The Infrastructure mode is similar to the structure of the mobile communications network: A special base station (Access Point) is used to coordinate the other network nodes (Clients). The base station sends small data packets (so called Beacons) in adjustable intervals (ten times per second by default) to all stations being in the footprint. The beacons contain among others the following information: Network name ("Service Set identifier", SSID), List of supported transfer rates, Type of encryption.

This beacons ease the connection establishment, because the clients just have to know the network name and optional some parameters for the encryption. The permanent sending of beacon-packets also allows a control of the reception quality - also when no user data are sent or received. The beacons are always sent with the lowest transfer rate (1 MBit/s), the successful reception of the beacons does not guarantee a steady connection to the network.

##### 3.5.8.2.2 Ad-hoc Mode

(Loose translation of an excerpt from the German version Wikipedia, the free encyclopaedia)

In the Ad-hoc mode (lat.: "created for this moment") no station is favoured; they all are on a par. Ad-hoc networks can be established quickly and without great effort. But for a spontaneous networking of a few terminals other techniques (Bluetooth, Infrared) are commonly used.

The preconditions for using the Ad-hoc mode are the same as for the Infrastructure mode: All stations use the same network name ("Service Set Identifier", SSID) and optionally also the same settings for the encryption. Because there is no central instance for this operating mode and because no beacon-packets are sent, a client cannot determine, whether there are other stations (using the same settings) within reach, who is part of the network or how good the connection quality is. Therefore, the Ad-hoc mode is suitable only for a small number of stations, that have to be close to each other because of the limited reach of the transmitter. Otherwise, it is possible, that a station cannot communicate with the other stations, because they simply do not receive a signal.

Forwarding data packets between the stations is not intended and not possible without further ado in practice, because in the Ad-hoc mode no information are exchanged, that might give the single stations an overview over the network. Gathering and exchanging these information is part of the upgrading of an Ad-hoc network to a mobile Ad-hoc network: Software components on each stations collect data (e.g. for visibility of other stations, connection quality etc.), exchange them among each other and make decisions concerning the forwarding of the user data. The development in this field is not finished yet. By now

a long list of experimental protocols (OLSR, MIT RoofNet, B.A.T.M.A.N etc.) and several proposals for standardisation (Hybrid Wireless Mesh Protocol, 802.11s) as well as some commercial solutions (e.g. Adaptive Wireless Path Protocol from Cisco) were produced.

### 3.5.8.2.3 Frequencies and ports

Channel Number	Frequency (GHz)	Permit in	Channel Number	Frequency (GHz)	Permit in
1	2,412	Europa, USA, Japan	8	2,447	Europa, USA, Japan
2	2,417	Europa, USA, Japan	9	2,452	Europa, USA, Japan
3	2,422	Europa, USA, Japan	10	2,457	Europa, USA, Japan
4	2,427	Europa, USA, Japan	11	2,462	Europa, USA, Japan
5	2,432	Europa, USA, Japan	12	2,467	Europa, Japan
6	2,437	Europa, USA, Japan	13	2,472	Europa, Japan
7	2,442	Europa, USA, Japan	14	2,484	Japan

Table 7: Frequencies and ports

### 3.5.8.2.4 Security and encryption

(Loose translation of an excerpt from the German version Wikipedia, the free encyclopaedia)

Part of the WLAN standard IEEE 802.11 is the Wired Equivalent Privacy (WEP), a security standard containing the RC4 algorithm. The contained encryption, with a static key of a length of just 40 bits (called 64 bits) or 104 bits (called 128 bits), sometimes also 232 bits (called 256 bits), does not guarantee, that the WLAN is secured sufficiently. By collecting pairs of keys Known-Plaintext-Attacks may happen. There are freely available programs, that are able to decrypt the password (a fast computer assumed), sometimes even without a complete packet cycle. Furthermore, each user of the network can read along the whole communication. The combination of RC4 and CRC is considered to be cryptographic insecure.

Therefore, technical complements were developed (e.g. WEPplus, Wi-Fi Protected Access (WPA) as advance and subset of 802.11i, Fast Packet Keying, Extensible Authentication Protocol (EAP), Kerberos or High Security Solution, that reduce the insecurity of WLAN more or less effective.

Child of the WEP is the new security standard 802.11i. It offers an increased security by using the TKIP (Temporal Key Integrity Protocol) for WPA or the AES (Advanced Encryption Standard) for WPA2. At the moment, it is regarded to be non-decipherable, as long as no trivial passwords are used, that can be decrypted via a dictionary-attack. It is recommended to create the passwords with a password generator, that contain special, numeric and alphabetical characters (upper and lower case) and have a minimum length of 32 characters.

CCMP (= Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) or also Counter-Mode/CBC-Mac Protocol is, according to IEEE 802.11i, a cryptography algorithm. CCMP is based on the Advanced Encryption Standard (AES) and uses a 128-bit-key with a 48-bit-initialisator for answer query.

### 3.5.8.2.5 Authentication

(Loose translation of an excerpt from the German version Wikipedia, the free encyclopaedia)

Extensible authentication Protocol is a protocol for authenticating clients. It can access to the RADIUS server for user administration. EAP is mainly used for large WLAN installations within WPA.

Encryption systems, that require, that both members know the keys before communicating (= symmetric systems), are called Pre-Shared Key (PSK). An advantage of the PSK encryption is, that it can be realized more easily between two known members than asymmetric encryption. The major disadvantage of this system is, that the two members have to exchange the key in private before the communication takes place. Therefore, the PSK system is not suitable for many applications in the internet (e.g. online shopping), because there the prior exchange of a key is impossible or far too extensive. In such a case it is easier to use the Public-Key system.

### 3.5.8.2.6 Passwords

(Loose translation of an excerpt from the German version Wikipedia, the free encyclopaedia)

Modern encryption system are technical advanced insofar as they often can only be decrypted via dictionary attacks (except from trying all possible keys = Brute-Force method). At both attacks the weak point is the password (key), set by the user. In order to create a password, that is not less insecure than the actual encryption (112 to 128-bit-key for current systems), theoretically a sequence of about 20 random characters is necessary. If no random characters are used, considerable longer passwords are necessary in order to guarantee the same security level.

The length of passwords, that can be used for encryption, is often limited by the software (e.g. using AES passwords with more than 32 characters do not increase the security). Therefore, you should always use combinations of characters, that consist of rare words or word orders, fantasy or foreign-language words, initial letters of a sentence, numeric and/ or special characters or even combinations thereof. Its components should be unforeseeable for an attacker, who is well-informed about the person and his/her interests. As alternative you can use a password generator and fix the password in you memory or you note it on a secret place.

A relatively secure password could be: 0aJ/4%(hGs\$df"Y! (16 characters). The major problem of such sequences using random characters is, that they are difficult to be kept in mind and therefore have to be noted somewhere. A simpler alternative is, to use a rehearsed sentence and to change some characters, e.g. "dIE bANANNE\*3 durch 1/4 nIKOTIN" (32 characters). It is very important to work in enough random characters. Suitable is the use of the initial letters of a sentence, e.g. "LS-Wbt7m/Ia1000tftY", created with the initial letters of the sentence "Little Snow-White beyond the 7 mountains/ Is a 1000 times fairer than You".

Although the use of special characters can increase the security, because the password becomes more complicated, you should use them carefully, if there is the possibility, that the password has to be used in foreign countries: It might be possible, that some special characters do not exist on foreign keyboards.

### 3.5.8.3 BIOS dialogue DatafoxStudioIV

In the BIOS dialogue of the Datafox Studio (< Communication => Device configuration BIOS >) you can make the same settings as directly on the terminal (except the restriction at TCP/IP Set default and Factory default WLAN, which is possible only at the terminal). You could compare the BIOS menu with a remote maintenance tool, but changing the settings is accessible only via RS232.

The setting of WLAN parameters is going to be available from version 04.01.06.xx in the Datafox Studio.

### 3.5.8.4 Dependencies

Because of the different methods for parameterisation, certain dependencies of several parameters arise.

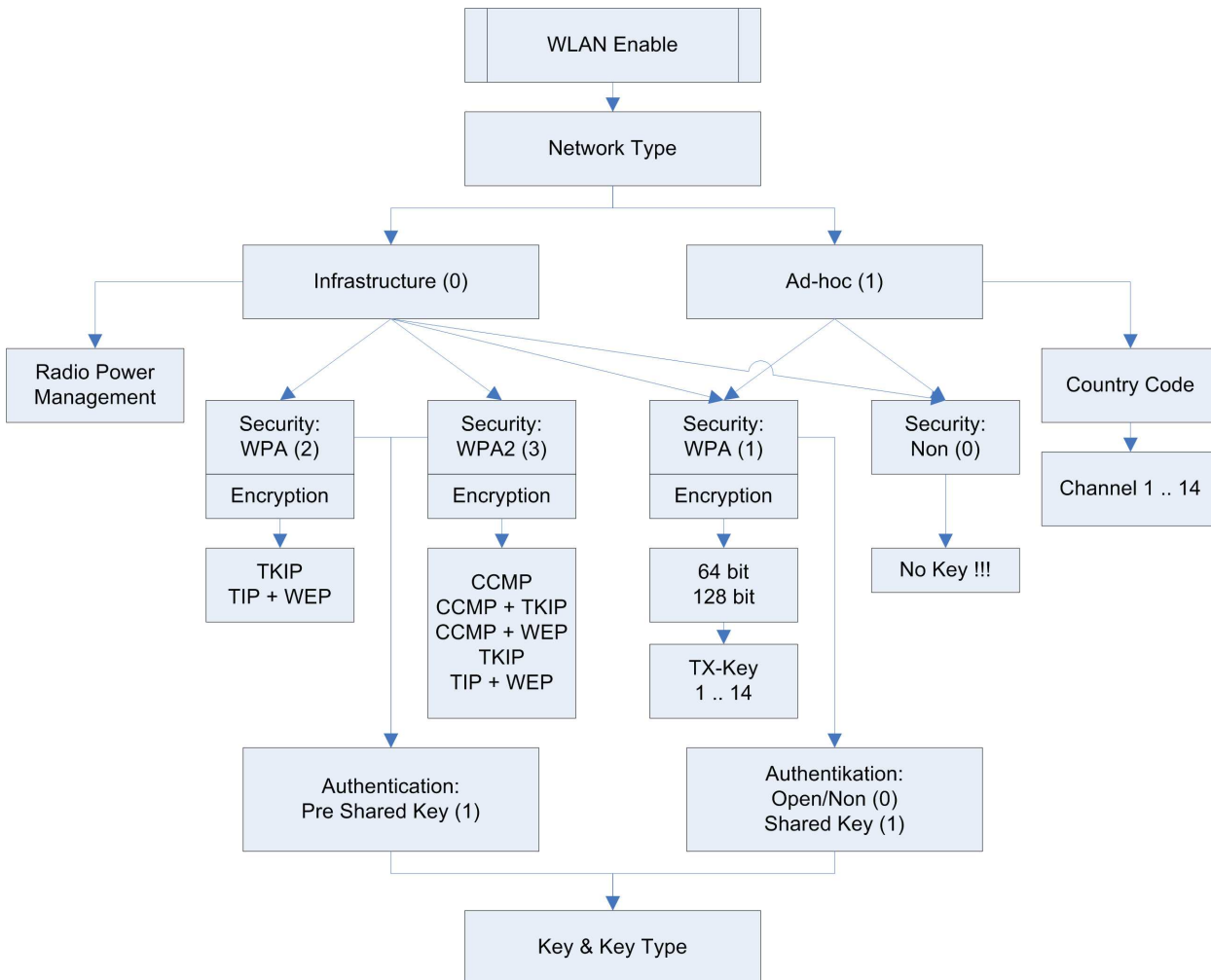


Figure 41: Dependencies

### 3.5.8.5 WLAN configuration via the Lantronix tool

You may find the device installer<sup>TM</sup> of Lantronix® on the enclosed Datafox product DVD under DVD:

Datafox-Optionen ( eingebaute Module )wLAN, Matchport.

With the help of this tool the COM servers Xport and MatchPort of the Datafox devices can be configured. The device installer accesses to the COM server via TCP/IP, the Datafox terminals via RS232. If a COM server is not available, because it is adjusted that much, so that the device installer is unable to access, it is possible to reset the COM server to the default values via the BIOS menu of the terminal.



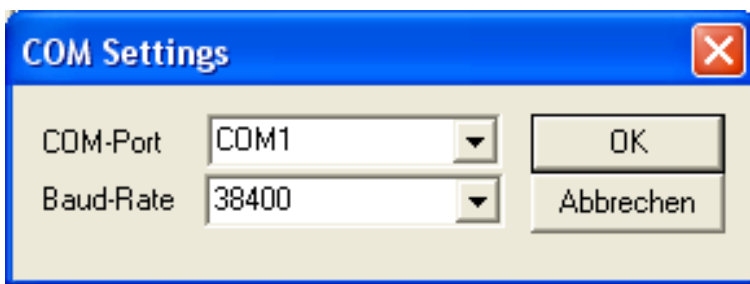
### 3.5.8.6 WLAN configuration via the DatafoxStudioIV

#### 3.5.8.6.1 General

The program WLANConfig can set the TCP/IP and the WLAN settings of the MatchPort via RS232. These settings can be saved as a file and the data of this file can be transmitted to the device. The dependencies of the single parameters among each other are permitted or locked by the program automatically. Four dialogues are provided for working with the program.

- ▶ WLAN settings (main dialogue)
- ▶ Selection of the serial interface (COM settings)
- ▶ Selection of the configuration file (Select INI-File)
- ▶ TCP/IP settings (Terminal TCP/IP settings)

#### 3.5.8.6.2 Selection of the serial interface



Via this dialogue you can select the interface of the PC, to which the MasterIV terminal is connected. Usually a baud rate of 38400baud is set, which has to correspond to that one of the terminal. You start the dialogue by pressing the button COM settings.

Figure 42: Selection of the serial interface

### 3.5.8.6.3 Selection of the configuration file

Via the button Select INI-File the dialogue is started. Here you can create new files or select a file, where data are logged on. On the INI file all settings of the TCP/IP and the WLAN are logged.

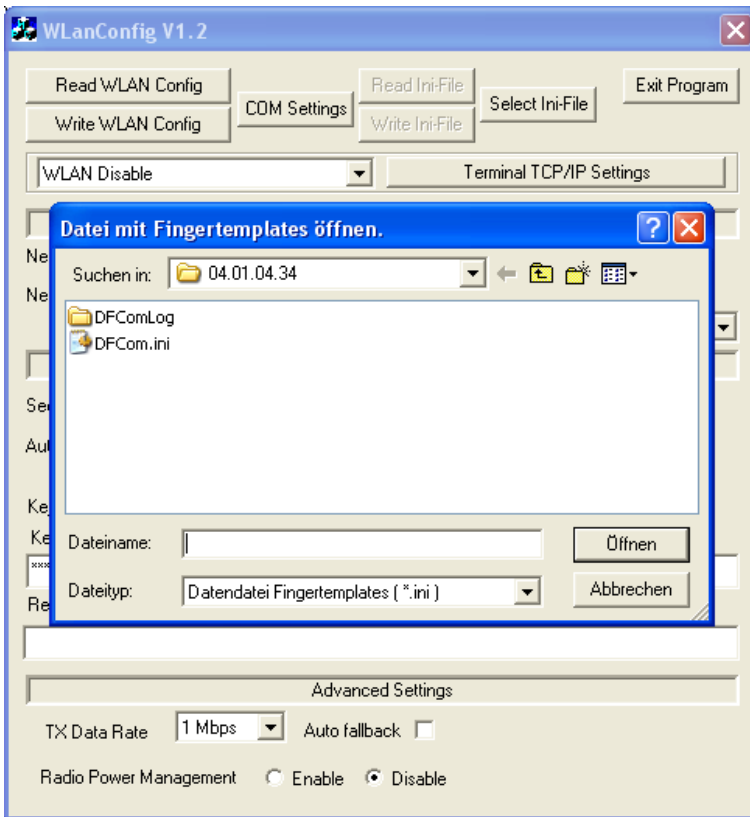
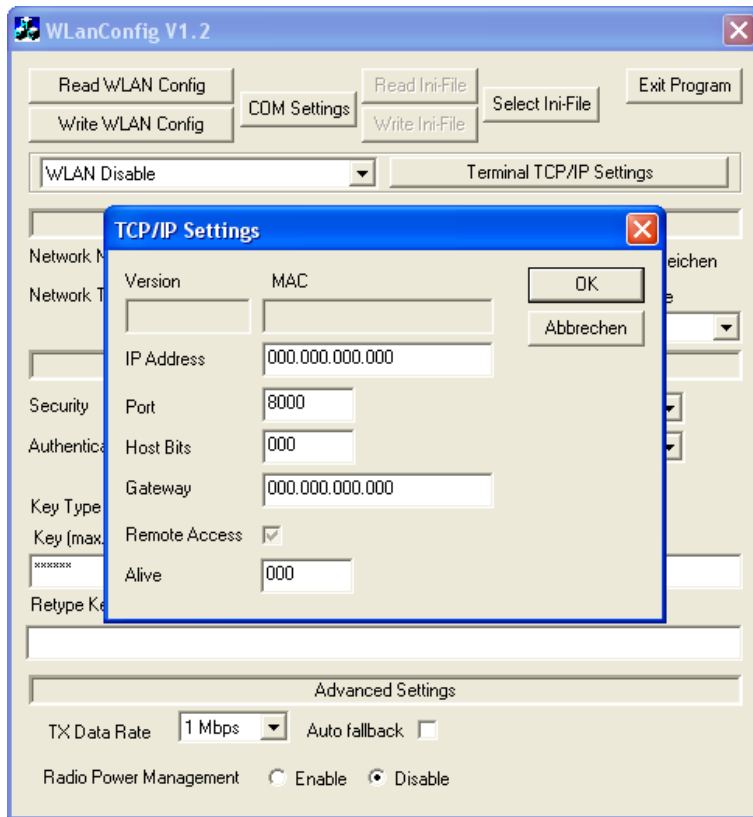


Figure 43: Selection of the configuration file

### 3.5.8.6.4 TCP/IP settings



Via the button Terminal TCP/IP Settings the dialogue is started. The current firmware version of the MatchPort and the MAC-address are displayed. You can edit the other parameters, which are equal to those of the BIOS dialogue of the terminal and of the Datafox Studio.

Figure 44: Selection of the configuration file

### 3.5.8.6.5 WLAN settings

The WLAN settings allow the editing of values, that were read out of the terminal and loaded in on a INI file or entered manually. It is very important, that the key cannot be read out of the terminal. It also cannot be re-recorded, if it was not entered. If the key is available in the INI file, a group of \* characters is displayed on the key-edit fields after loading the data. It is also transmitted to the device then. In order to use WLAN you have to set WLAN Enable. This parameter can also be set by the device installer of Lantronix. If you want to configure several devices via WLANConfig, you have to note, that the IP-address of the devices has also to be set.



**Caution:**

After transmitting the parameters the device has to be set from RS232 to TCP/IP, so that the MatchPort is activated. Only then it is available in the network.

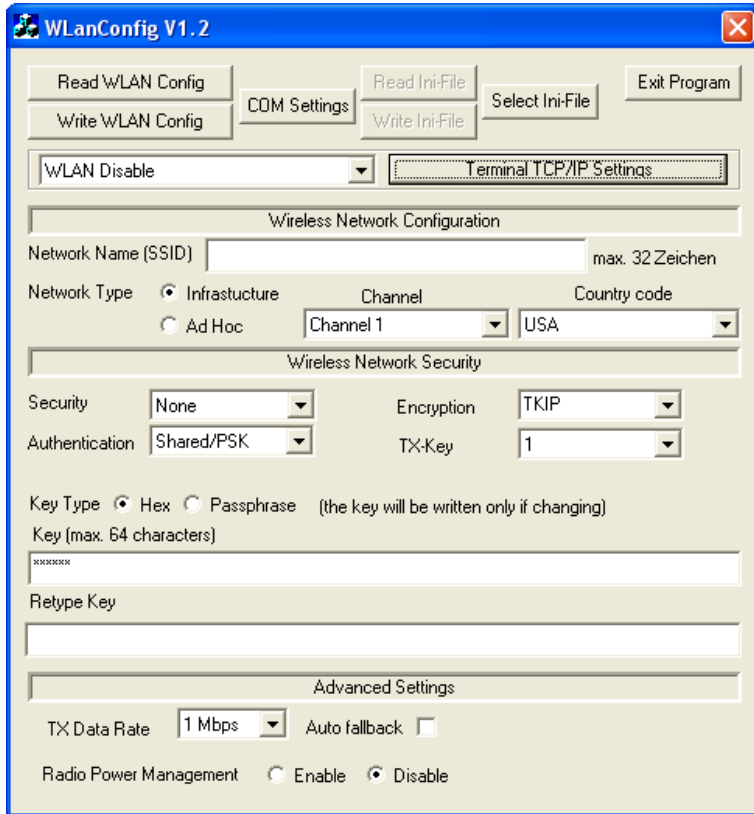


Figure 45: Selection of the configuration file

Via Read WLAN Config the data are loaded from the device to the program.

Via Write WLAN Config the data are loaded from the program into the device.

Via Read INI file the data are loaded from the selected file into the program.

Via Write INI file the data are written from the program in the file.

### 3.6 Access control II with TS TMR33 modules

The following hardware is available to construct an access control with TS TMR33 modules. The different options can be combined with each other according to the hardware requirements of the single devices.



#### ZK-MasterIV

Because the ZK-MasterIV is only used for the access control, door and remote monitoring, you can supervise up to 16 doors with one device and control 18 doors at most.



#### Türmodul (TS TMR33-TM)

72 x 72 x 40 mm

The door module is offered as pure electronic component e.g. to build it in a patress box, or in a housing for surface mounting with alarm control panel.



#### Reader (TS TMR33-L)

80 x 80 x 25 mm

The reader can be ordered separately to connect it directly to a PC or another access check. A connecting diagram and a description of the commands for the activation are included.



#### Module set = reader + door opening function (TS TMR33-LTM)

80 x 80 x 25 mm

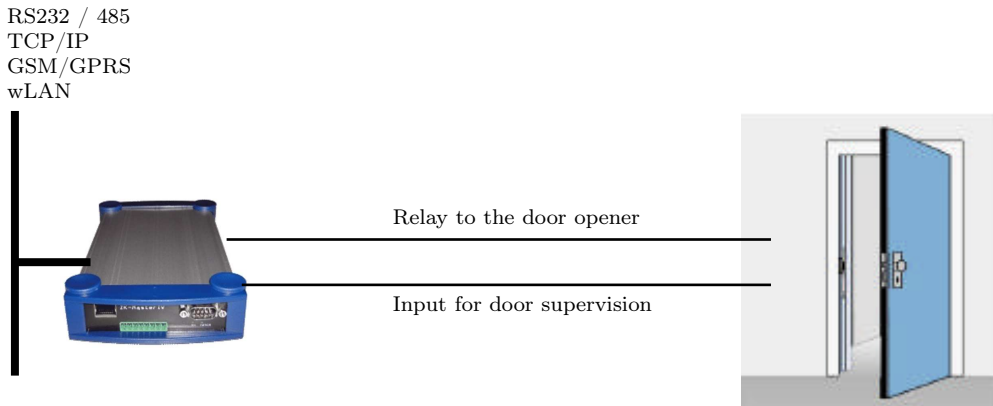
The module set can be ordered separately to connect it directly to a PC or another access check. A connecting diagram and a description of the commands for the activation are included.

#### 3.6.1 Set-up

In the following chapters different possibilities to set the device up are explained. The ZK-MasterIV is used as reference device.

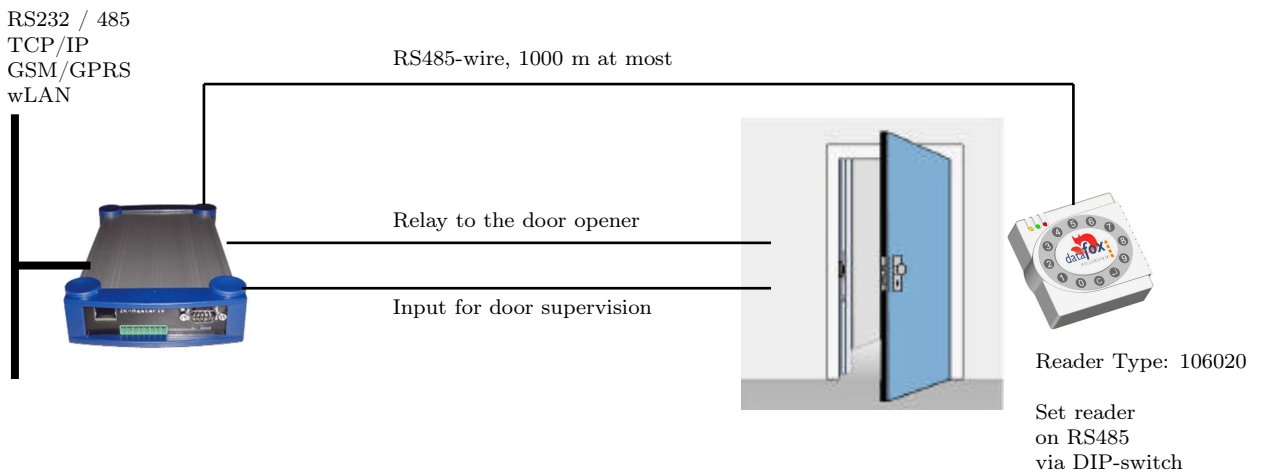
### 3.6.1.1 A door without a separate reader

The time recording terminal is access scanner, access master and door-opener at the same time. This solution should only be used in protected places so that the door opening relay cannot be manipulated.



### 3.6.1.2 A door with a separate reader

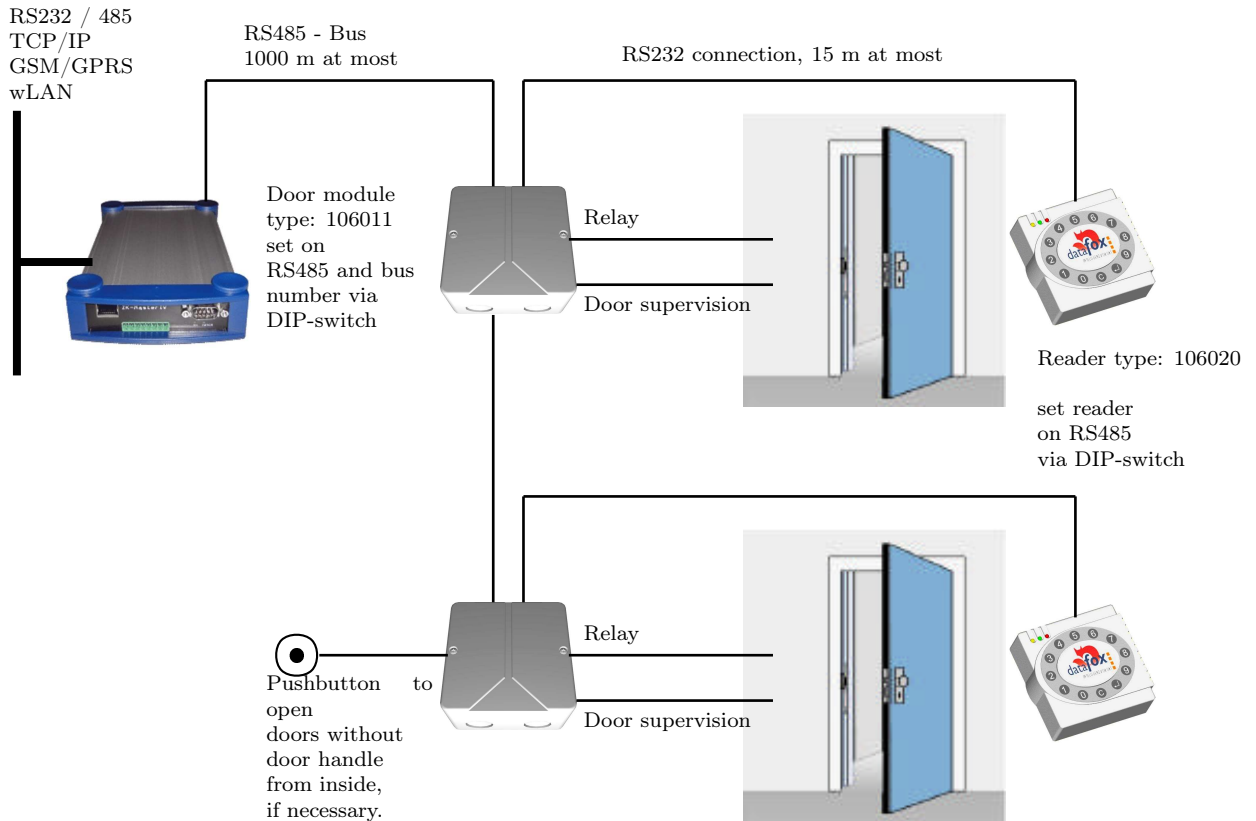
The ZK-MasterIV is installed in a protected area inside a building and the reader is installed outside. The terminal is access master and door-opener at the same time. The door opening relay is in the ZK-MasterIV and thus in the protected area. The access identification captured by the reader is transmitted to the ZK-MasterIV and analysed by it. If the access is permitted, the door is opened via the relay in the ZK-MasterIV.



This version is used frequently and can be installed easily and economically as shown in the figure above.

### 3.6.1.3 Several external doors via RS485 bus

Here a door module has to be used so that the door opening relay is in the protected area.



The door module permanently calls up the reader. If a transponder is read the information is transmitted from the reader to the door module. The ZK-MasterIV permanently polls to the door module. If a booking is available, it is collected immediately. If the access is permitted, the ZK-MasterIV sends a command to the door module to open the door.

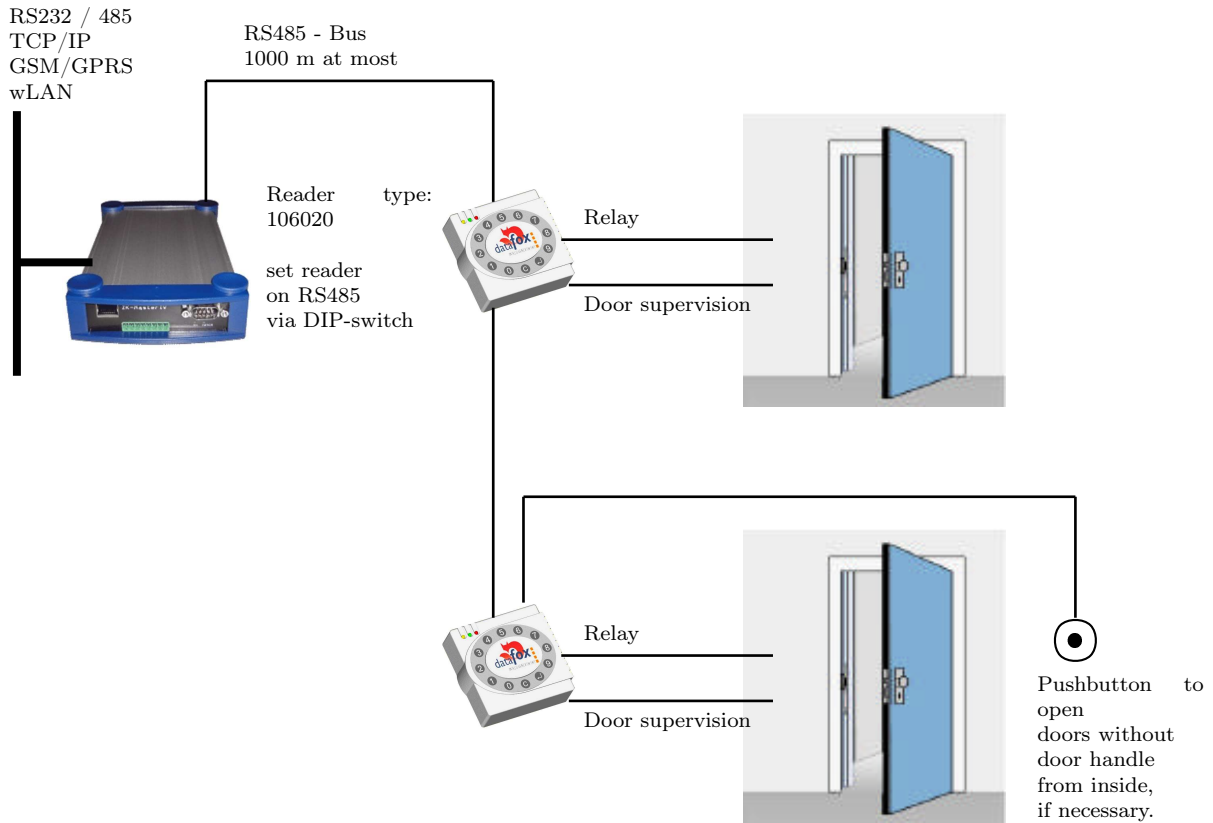


**Note:**

The relay in the ZK-MasterIV can be used here as well. See chapter 3.1, that means the terminal can replace the first door module. In order to use the appropriate reader in the RS485 bus, it has to be set on RS485 via the DIP switches at the backside of the reader.

### 3.6.1.4 Several internal doors via RS485 bus

The combined reader + door-module is used here. The door opening relay is included in the combined module. Watch out, this assembly must not be used at outdoor locations because then the relay is not in a protected area.



The ZK-MasterIV permanently polls to the door module. If a booking is available, it is collected immediately. If the access is permitted, the ZK-MasterIV sends a command to the door module to open the door.



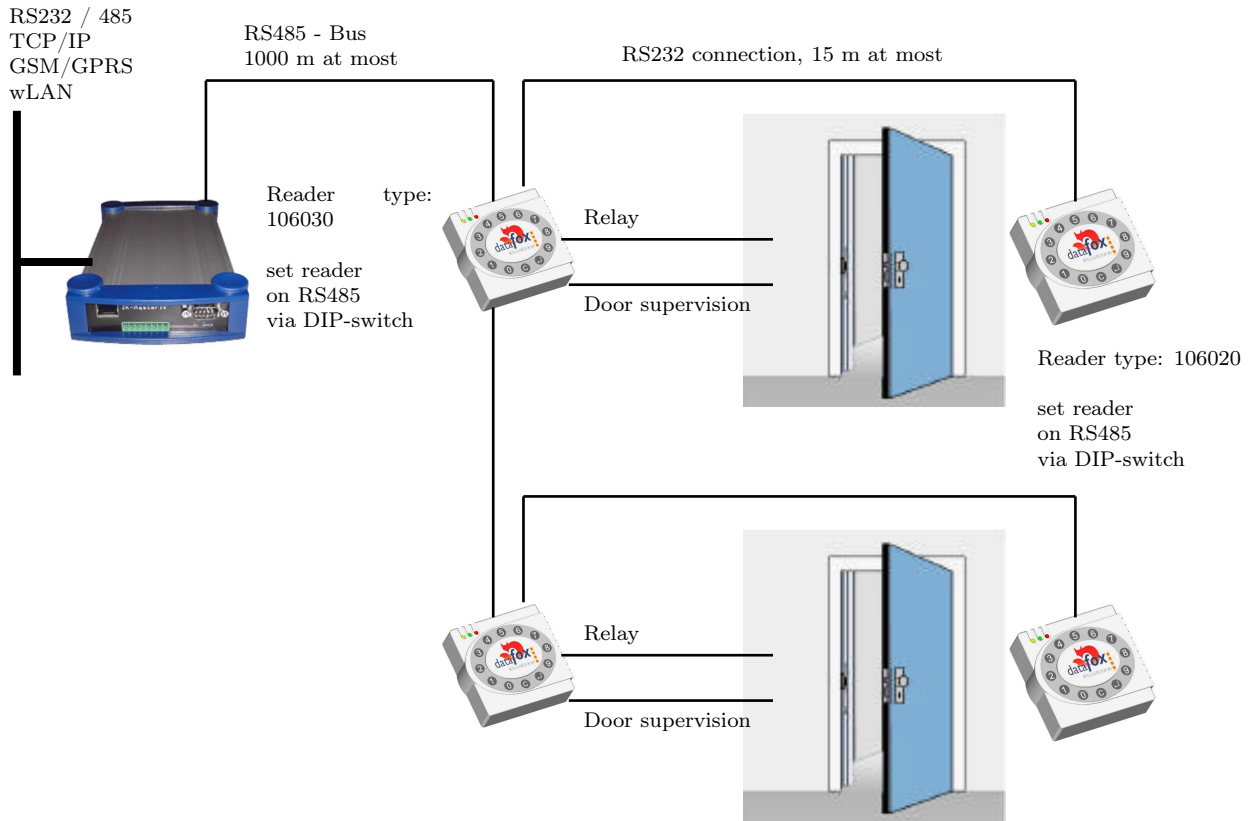
**Note:**

The relay in the ZK-MasterIV can be used here as well. See chapter 3.1, that means the terminal can replace the first door module. In order to use the appropriate reader in the RS485 bus, it has to be set on RS485 via the DIP switches at the backside of the reader.



### 3.6.1.5 Mantrap function with RS485 bus

The combined reader + door-module and the reader-module is used here.



The ZK-MasterIV permanently polls to the door module. If a booking is available, it is collected immediately. If the access is permitted, the ZK-MasterIV sends a command to the door module to open the door.



**Note:**

The relay in the ZK-MasterIV can be used here as well. See chapter 3.1, that means the terminal can replace the first door module. In order to use the appropriate reader in the RS485 bus, it has to be set on RS485 via the DIP switches at the backside of the reader.

### 3.6.2 Connection

The following figure shows the possibilities for connecting the TMR33 devices to a ZK-MasterIV for the access control. The TMR33 devices have to be set depending on the interface that is used (RS232 or RS485).

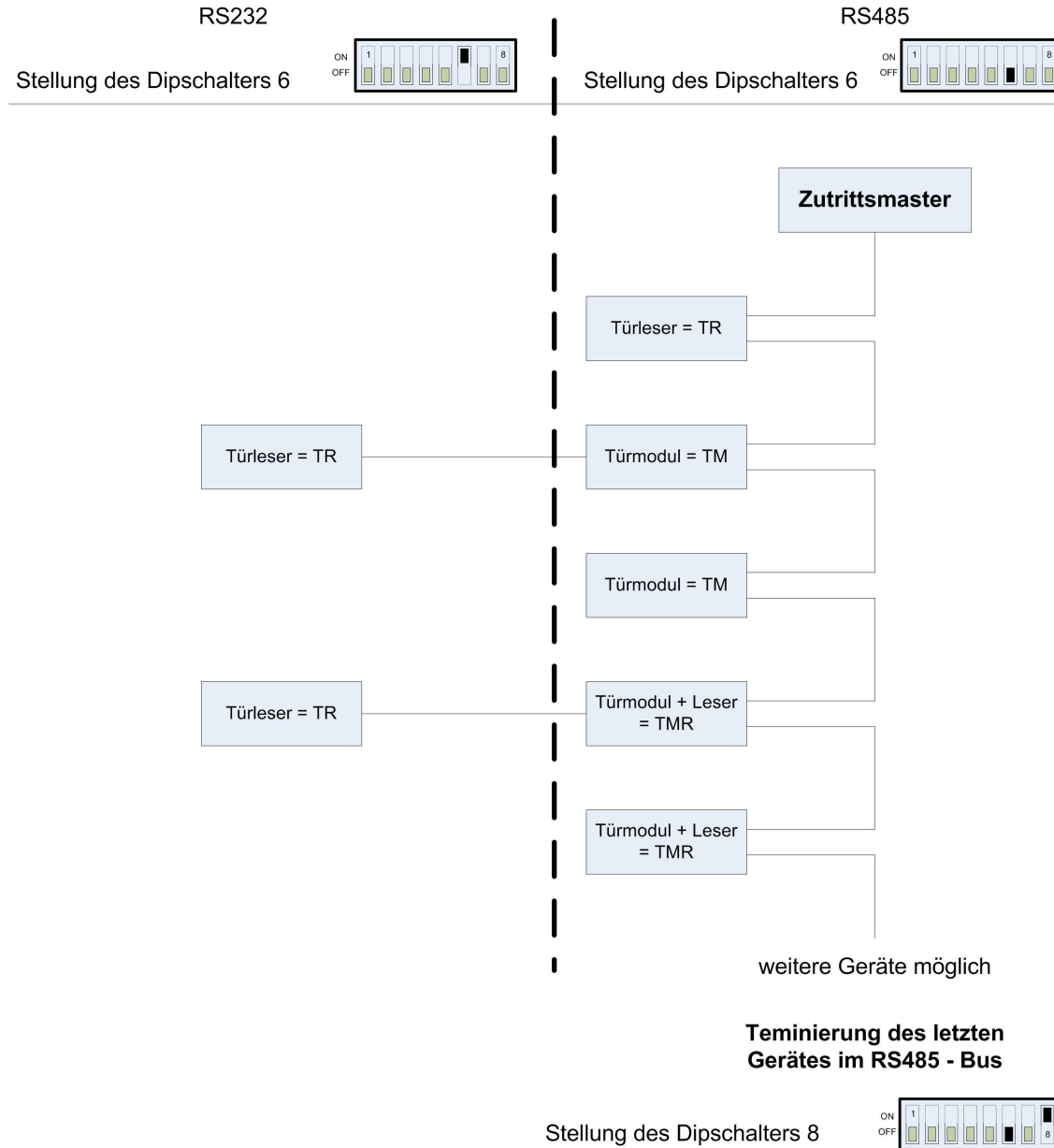


Figure 46: Connection of the access control II

The DIP switches 1 - 5 are for the bus configuration. Via them the bus number of the device is set. The DIP switch 1 in position "ON" and 2 - 5 in position "OFF" stand for bus no. "1". The DIP switches 1 and 2 in position "ON" and 3 - 5 in position "OFF" stand for bus no. "3".



**Caution:**

The installation and connection of the TMR33 module may only be carried out by a person qualified in this field. Avoid switching the connecting terminal (reverse polarity).

From this arise different possible combinations. The following figures show examples for the connection wiring.

**3.6.2.1 Wiring**

In most cases a shielded twisted pair cable is used as transmission medium for the assembling of a RS485 bus. It should be a twisted pair cable because that way the voltages induced by an electromagnetic field work opposite and thus offset each other.

In accordance with the specifications (TIA-EIA-485-A) the maximum cable length depends on the transmission rate.

<b>length of segment [m]</b>	100	200	400	1000	1200
<b>data rate [kBit/s]</b>	12000	1500	500	187,5	9,6

Table 8: Cable length dependent from the data rate

Our recommendations for a data cable are the following types of cables: Li-YcY 2x2x0,5 mm<sup>2</sup>, J-2YY 2x2x0,5 mm<sup>2</sup> oder J-Y(ST)Y 2x2x0,5 mm<sup>2</sup> (Cat5 shielded).



**Caution:**

When erecting an access control system, a calculation of the maximum cable length, the necessary cable cross-section and voltage supply has to be done in any case. See chapter 3.6.2.2 for further hints.

**Example:** Wiring for a door

An external access reader TS TMR33-L is connected directly to the terminal. The door opening is controlled via the relay integrated in the terminal. Further functions, e.g. supervision of the door (open or closed), can be realized via the digital inputs of the ZK-MasterIV.

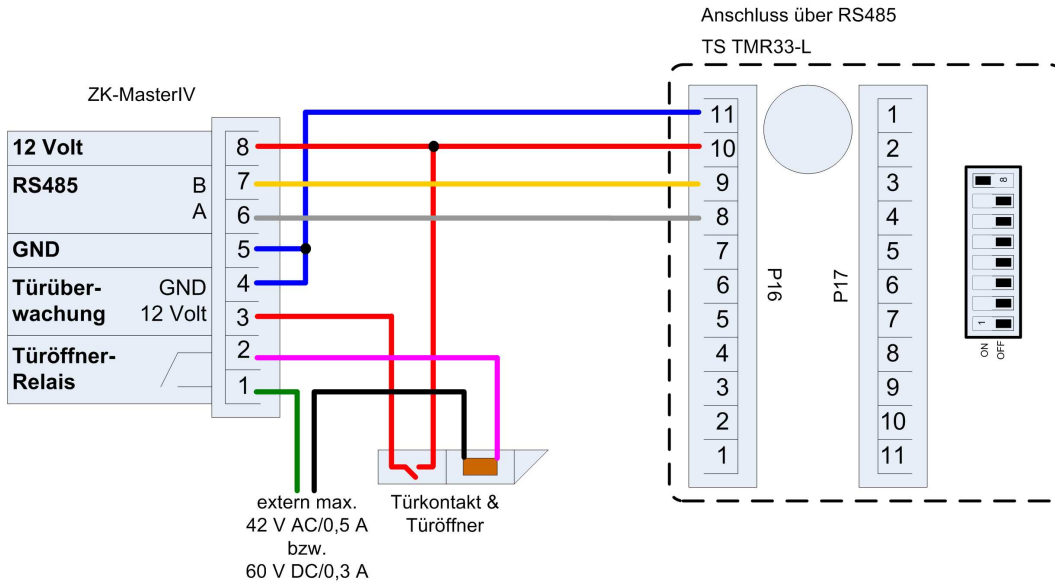


Figure 47: Wiring for a door

In this case the reader table (access control list) has to be configured as follows:

ID	ZM	TM	RefLocation	RefAction	PinGeneral
1	1	320	0	1	0
2	1	000	0	1	0

Table 9: Reader table

ID = 1 identifies the data record for the ZK-MasterIV, that always gets the value 320 in the column TM (Türmodul/ door module). ID = 2 identifies the external reader (TS TMR33-L), that is connected to the ZK-MasterIV via RS485. The type of connection (RS485) is marked by the zero at this position 000 in the column TM.

**Example:** Wiring of a mantrap

A door is controlled via an internal door module with integrated reader TMR33-TMR and an external access reader TMR33-TR as mantrap. In this case the internal door module is connected to the ZK-MasterIV via a RS485 bus. The external access reader is connected to the internal door module with a RS232 stub. The door opening is controlled via the relay integrated in the door module TMR33-TMR. In this case the door module with the relay is in the secure area and the external access reader without a relay is in the insecure area.

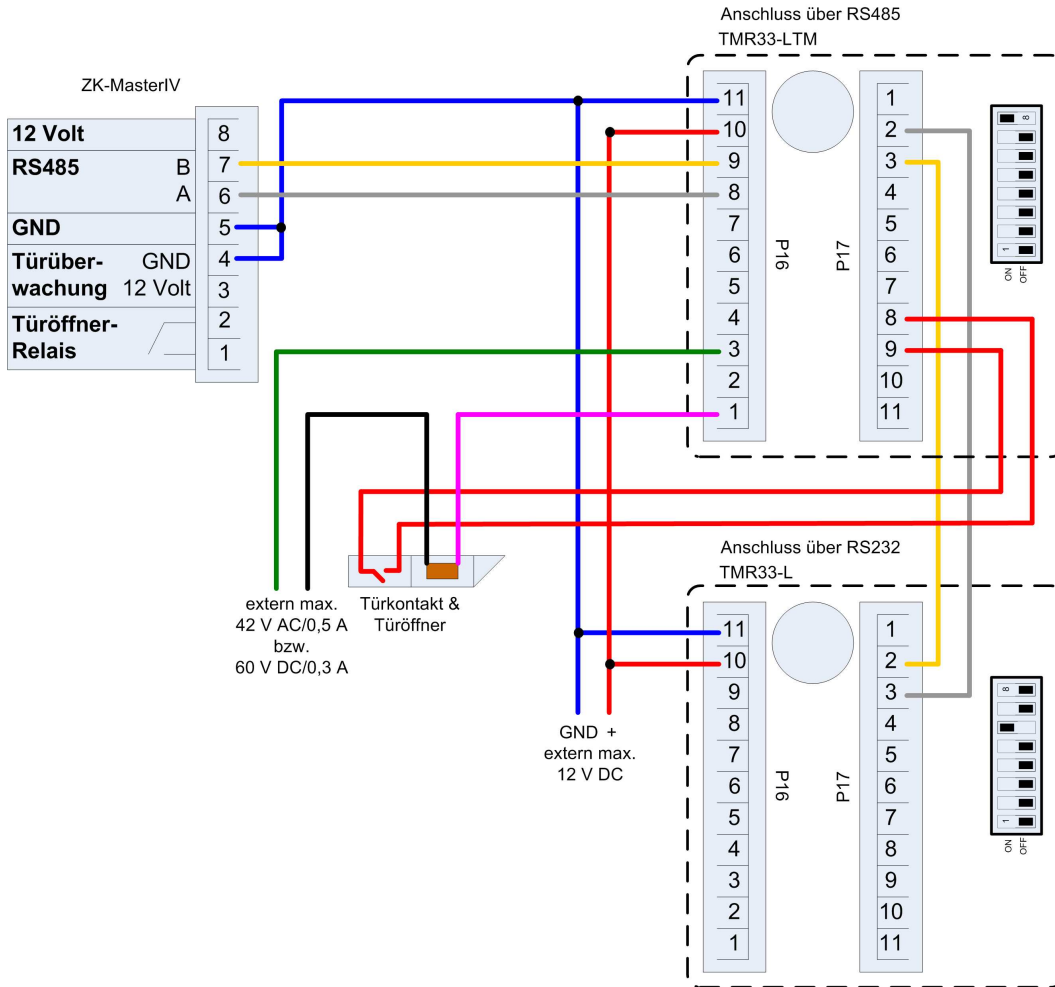


Figure 48: Wiring of a mantrap

	<p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• Connection for electricity supply via power supply unit or bell transformer. Please note the hints for the calculation of the cable cross-section and the cable length.</li> <li>• Install the door-opener in the protected area when using it for exterior doors.</li> <li>• At closed door contact approx. 15 mA are used up at 12 V = 0,18 Watt. This means a consumption of approx. 1,6 kWh per year.</li> </ul>
--	---

**Example:** Controlling the door-opener only via the ZK-II You can control the door-opener directly via the access control-II (ZK-II). Please note that the door-opener has to work in a voltage range from 8 to 12 V DC and must not exceed a power consumption of 100 mA.

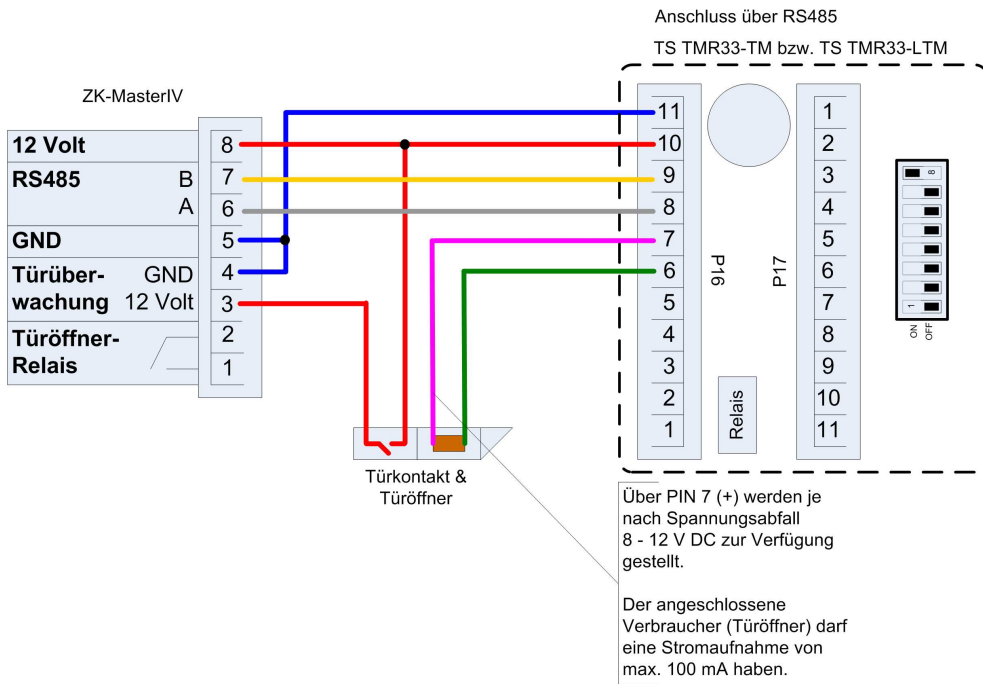


Figure 49: Controlling the door-opener via ZK-II

**Example:** Controlling the door-opener via the ZK-II and a push-button It is possible to additionally connect a push-button for controlling the door-opener.

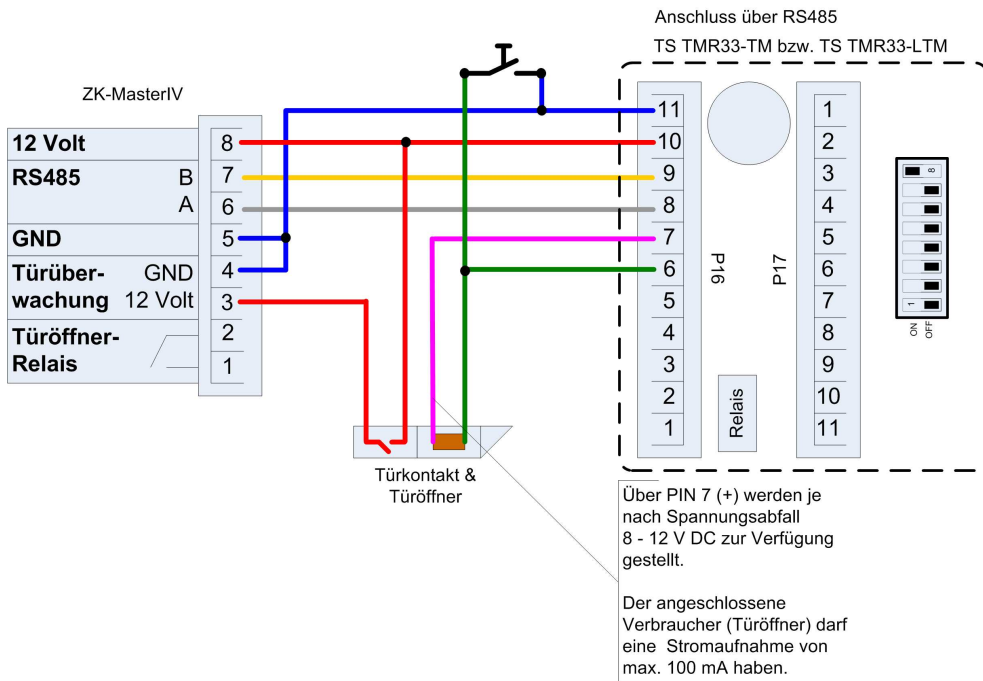


Figure 50: Controlling the door-opener via the ZK-II and push-button

**Example:** Controlling the door-opener via the ZK-II, relay and push-button

You want to control the door-opener directly via the access control-II. You want to open the door without transponder via a push-button in a lobby with a view of the entrance area. Additionally, this push-button circuit should only be active at certain times. This scenario can be portrayed as follows:

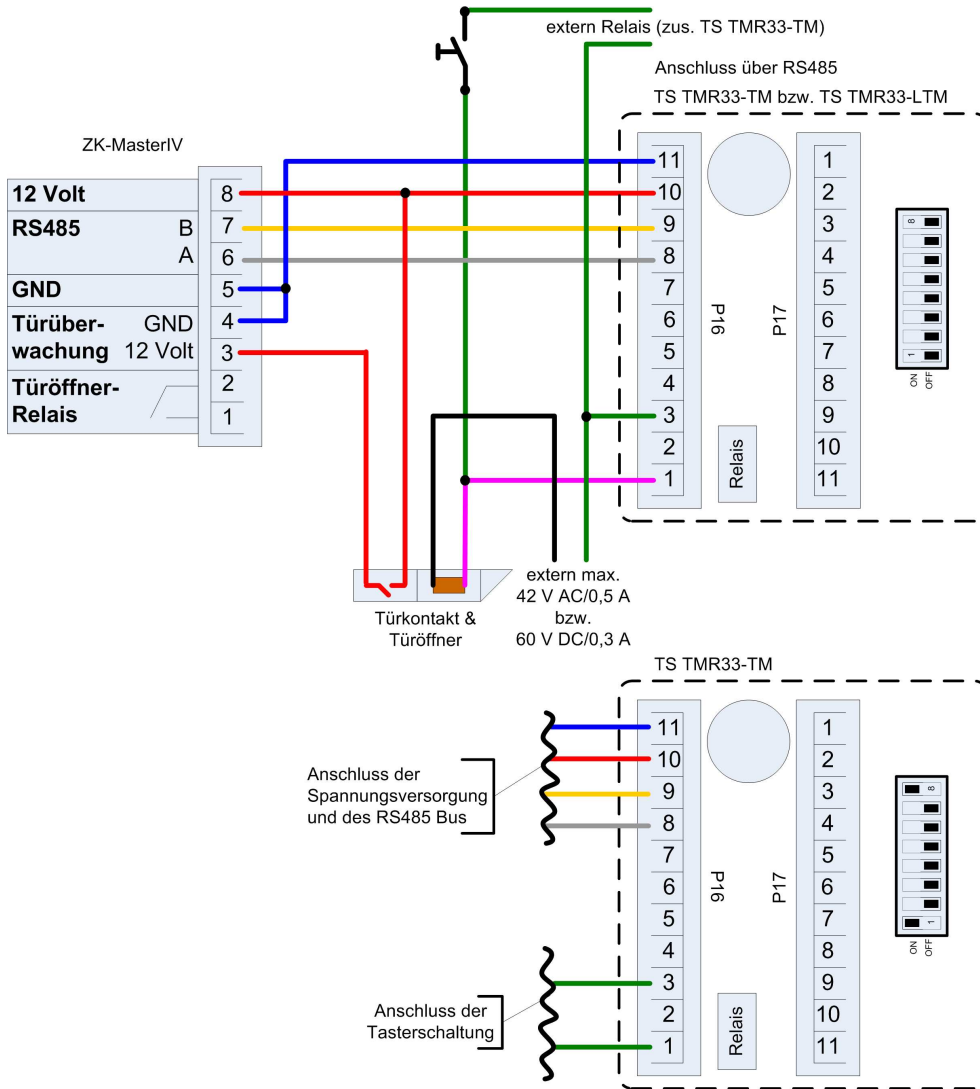
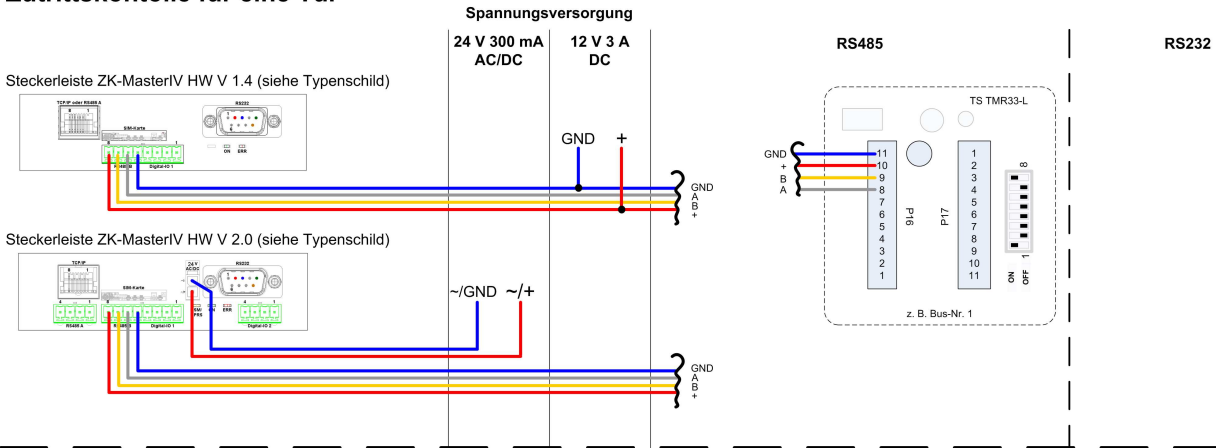


Figure 51: Controlling the door-opener via the ZK-II, the relay and a push-button

Initially, we use an external voltage source for the supply of the door-opener. It is controlled via the relay of the TS TMR33-TM, connection 1 and 3 of the strip terminal P16. The NC contact of the relay is bridged with the push-button. The activation of this push-button circuit is realized via an additional relay (TS TMR33-TM). You can configure the period of time of the activation at the access control lists in the ZK-II. For this you have to include the additional TS TMR33-TM module in the reader table. In the action table you set which output (relay) is switched on which module of the reader table. Set the elapse-value on 0. You define via the reference on a time model (RefTime) from when the relay switches (push-button circuit activated) and when the relay drops out again.

Zutrittskontrolle für eine Tür



Zutrittskontrolle für mehrere Türen

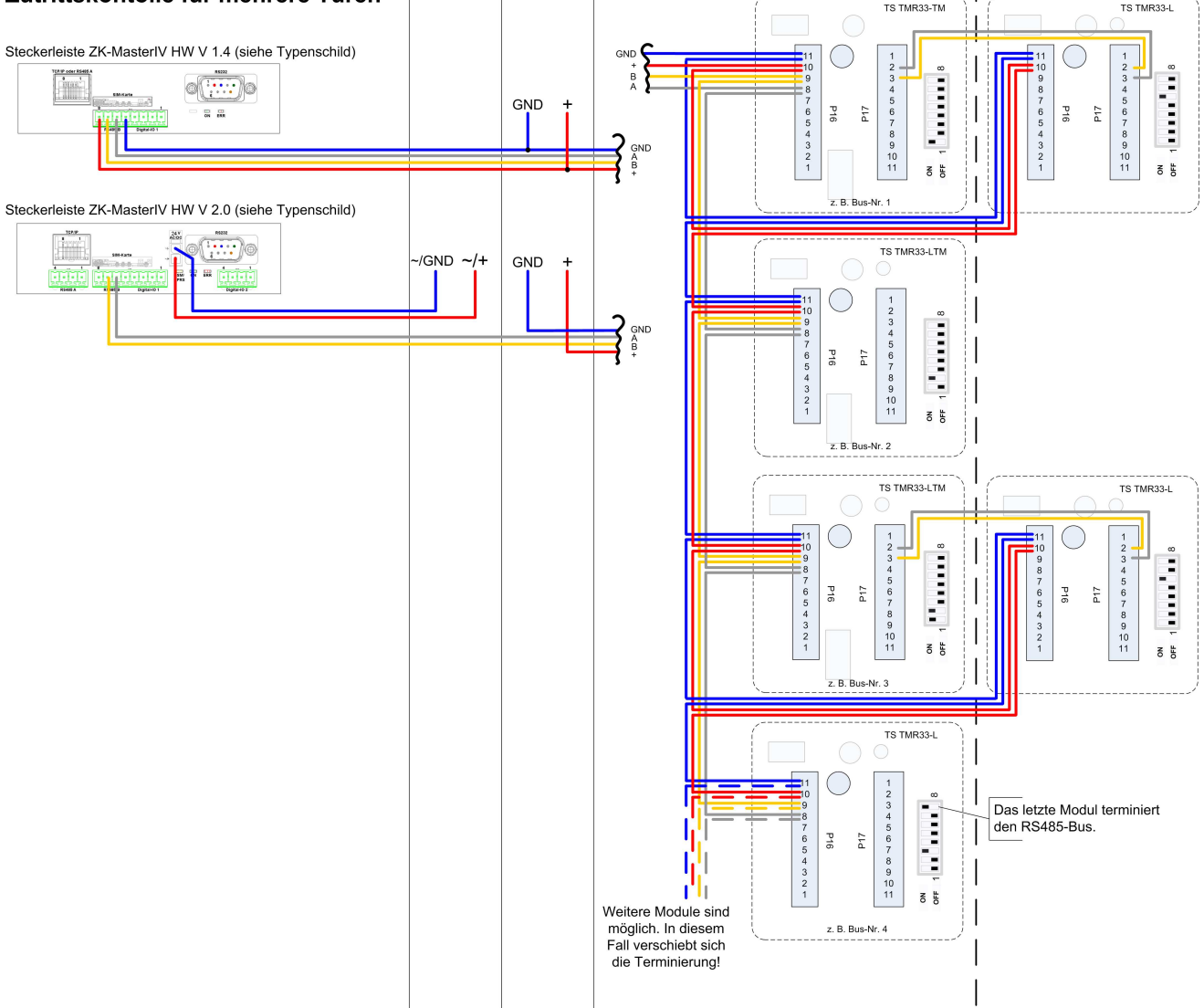


Figure 52: Wiring scheme



### 3.6.2.2 Calculation instructions

When using Datafox access readers or door modules, the necessary cable cross-section has to be calculated before setting up a RS485 network for the access control. The voltage drop in the whole bus must not be higher than 4 V. Please note that if you use a Datafox device power supply unit as voltage source, 16 modules at most (8 in the RS485 bus and 8 via RS232 stub line) can be fed.

#### Maximum power consumption of the single modules:

TS-TMR33-TR	56,5 mA
TS-TMR33-TM	156,0 mA
TS-TMR33-TMR	180,0 mA

The result of it is a permissible maximum power consumption per Datafox device power supply unit of (8 x 180,0 mA + 8 x 56,5 mA) 1,9 ampere. In order to assure this, you can calculate the necessary cross-section for a given cable length or the permissible maximum cable length for a given cable cross-section.



#### Caution:

Before a setting up and commissioning of a ZK-network, in any case the calculation has to be done by a person qualified in this field.

The cable cross-section is calculated as follows:

$$q = \frac{2 * I * l}{\kappa * U_v}$$

$q$  = Cable cross-section in  $mm^2$

$I$  = Current in A

$l$  = Cable length in m

$\kappa$  = Conductivity (kappa) for Cu-conductor =  $56 \frac{m}{\Omega * mm^2}$

$U_v$  = Voltage drop 4 V at most

Thus the developed equation for calculating the maximum cable length for a given cable cross-section is:

$$l = \frac{q * \kappa * U_v}{2 * I}$$

### 3.6.2.3 Topologie

If a bus topology is used when setting up the network, you have to calculate the cable cross-section for each bus segment with regard to the maximum power consumption of the respective segment (see figure 53).

At a star cabling the cable cross-section for each cable has to be calculated with regard to of the power consumption of the respective module.

**Note:**

Because this document only deals with the voltage supply of an access control system, the depiction of the RS485 data bus is abandoned in the figures. The voltage supply is simply depicted as one line. Additionally, the cable length that has to be calculated is marked by a broken line.

### 3.6.2.4 Examples

#### 3.6.2.4.1 Bus topology

We take as a basis that the longest distance from the voltage source to the last module is 65 m.

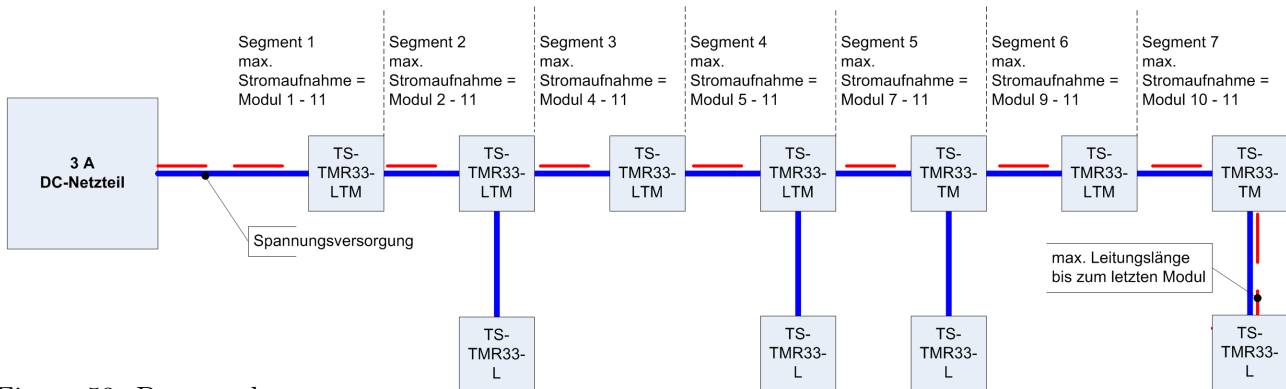


Figure 53: Bus topology

In order to assure a high safeguarding and to keep the calculation simple, you can take the following steps. Calculate the power consumption of all modules connected to a voltage source (max. 16 modules) and take the longest distance from the voltage source to the last module. If the result of this simplified method of calculation for the cable cross-section is a value higher than  $1,5 \text{ mm}^2$ , you have to use additional power supply units and recalculate the system. By this additional power supply unit you can compensate the voltage drop at a smaller cable cross-section by a shorter cable length (two sub-networks with regard to the voltage supply not with regard to the RS485 data bus). The calculation of the total power consumption for the example in figure 53 is as follows.

$$I = (4 * 56,5 \text{ mA}) + (2 * 156,0 \text{ mA}) + (5 * 180,0 \text{ mA}) = 1.438 \text{ mA} = 1,438 \text{ A}$$

Now we put the values in the equation and get the necessary cable cross-section:

$$q = \frac{2 * 1,438A * 65m}{56 \frac{m}{\Omega * mm^2} * 4V} = \frac{2 * 1,438A * 65m * V * mm^2}{56m * 4V * A}$$

$$q = 0,83mm^2$$

If we take as a basis that the bus has a maximum length of 200 m, the result of the calculation will be a cable cross-section of 2,6 mm<sup>2</sup>. That means we would need an additional power supply unit.

### 3.6.2.4.2 Star topology

In this example the maximum cable length for each cable is calculated separately for a given cable cross-section. We take a cable cross-section of 0,75mm<sup>2</sup> as a basis. The length of each cable has to be calculated separately.

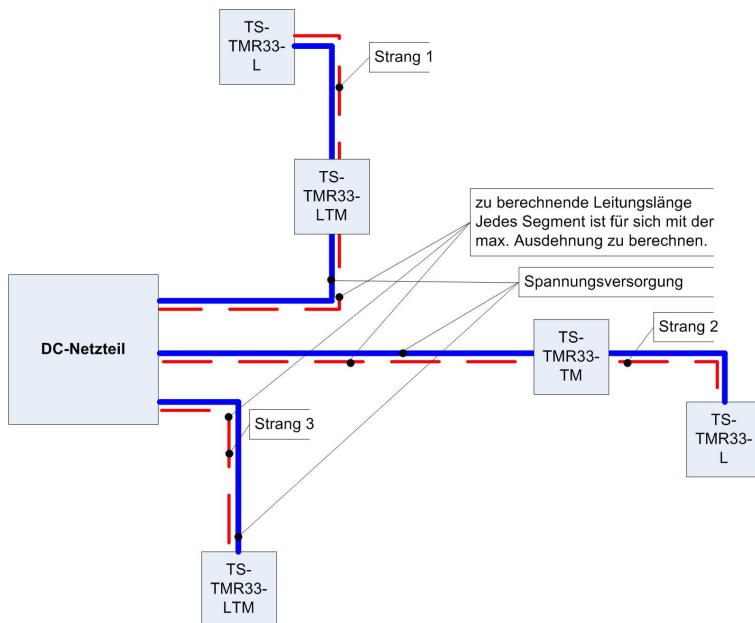


Figure 54: Star topology

**cable 1:**

$$I = 1x180,0mA + 1x56,5mA$$

$$I = 236,5mA$$

$$I = 0,2365A$$

The result for the maximum cable length for cable 1 is:

$$l = \frac{0,75mm^2 * 56 \frac{m}{\Omega * mm^2} * 4V}{2 * 0,2365A} = \frac{0,75mm^2 * 56m * 4V * A}{2 * 0,2365A * V * mm^2}$$

$$l = 355,2m$$

**cable 2:**

$$I = 1x156,0mA + 1x56,5mA$$

$$I = 212,5mA$$

$$I = 0,2125A$$

The result for the maximum cable length for cable 2 is:

$$l = \frac{0,75mm^2 * 56 \frac{m}{\Omega * mm^2} * 4V}{2 * 0,2125A} = \frac{0,75mm^2 * 56m * 4V * A}{2 * 0,2125A * V * mm^2}$$

$$l = 395,3m$$

**cable 3:**

$$I = 180,0mA$$

$$I = 0,18A$$

The result for the maximum cable length for cable 3 is:

$$l = \frac{0,75mm^2 * 56 \frac{m}{\Omega * mm^2} * 4V}{2 * 0,18A} = \frac{0,75mm^2 * 56m * 4V * A}{2 * 0,18A * V * mm^2}$$

$$l = 466,7m$$

**Note:**

The total power consumption has to be calculated for each cable.

**3.6.3 Configuration**

The basis of the access control II are tables. They store all information about the hardware configuration of the access control system, access right of the staff, periods of time (activation, blocking times, holidays,...). There is the following connection between the tables:

The tables are created as text files. For an easier administration you can add comments within the files.

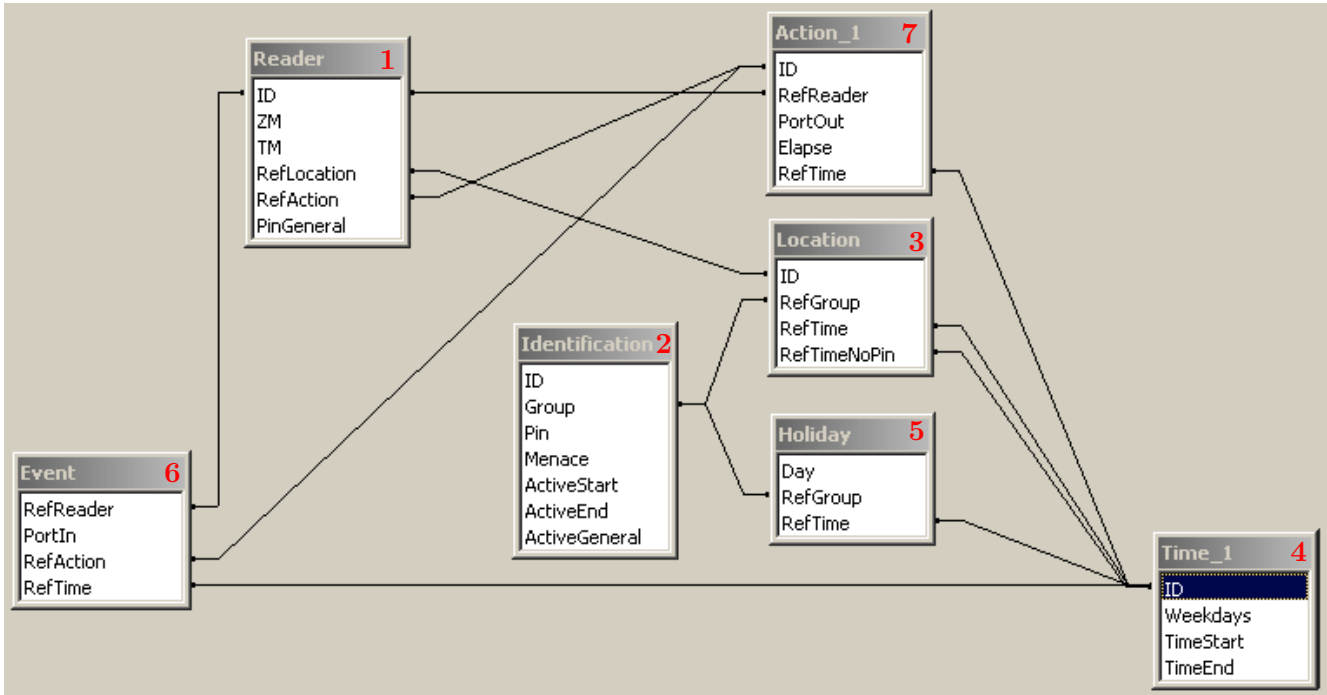


Figure 55: Data structure of the access control II

When adding comments you have to notice that in a comment line no field values can be given and that the comment line has to start with a semicolon.

A Reader.txt (Reader table) could look as follows:

```

; Reader list for the test access control system
; ID ZM TM RefLocation RefAction PinGeneral
1 1 320 1 1 0
2 1 010 1 1 0
    
```

Please gather a close description of the table structure, indication of the data types and field length from the following tables.

Alias	Data type	Length	Description
ID	Number (int)	4	Unique Key ( <i>Wert</i> > 0) of the Reader table.
ZM	Number (int)	4	It has in our example number 1. If there are several PZE-MasterIV in an access system, they can be depicted in one table connection and it is not necessary to have a separate string for each PZE-MasterIV.
TM	Number (int)	3	Contains two information in one number. Both figures on the left (010) indicate the bus number of the door module, the figure on the right (010) contains information about the type of connection. A 0 means a connection via RS485, a 1 stands for a connection via RS232 as stub.
RefLocation	Number (int)	4	Indicates which room is supervised by the reader.
RefAction	Number (int)	4	Indicates which action is worked through after a successful check.
PinGeneral	Number (int)	8	Can contain a numerical sequence via which a person without a card gets access.

Table 10: Reader table (list of all devices installed in the system - master and door modules)

Alias	Data type	Length	Description
ID	String (ASCII)	20	Contains the card no. which is read at the TMR33 device or terminal. A card can occur several times (is assigned to several authority groups).
Group	Number (int)	4	Assigns the card to an authority group.
Pin	Number (int)	8	Activates a PIN query if not equal 0. Please note that a PIN must not start with a zero. 0815 would be invalid.
Menace	Number (int)	4	Activates (if not equal 0) a "menace-PIN" that can be added to the PIN. If entered, the system sends a data record that can be analysed by software developed for this purpose and sets off the alarm.
ActiveStart	String (Date)	10	The tag entered here indicates the beginning of validity of the card.
ActiveEnd	String (Date)	10	The tag entered here indicates the end of validity of the card (e.g. 2007-07-12 = yyyy-mm-dd).
ActiveGeneral	Number (int)	1	Activates or deactivates this card record. 0 = card blocked 1 = card active 2= virtual card (use only via DLL) 3 = access only by entering the PIN 9 = general authority (no PIN query)

Table 11: Identification table (list of all cards known by the system))

Alias	Data type	Length	Description
ID	Number (int)	4	ID of the room. All other tables refer to this data line via this number, if necessary.
RefGroup	Number (int)	4	Reference to the identification table. Labels the access authorized group. All cards of this group have access to this room.
RefTime	Number (int)	4	The time model in which authorized persons get access. (0 = not used)
RefTimeNoPin	Number (int)	4	The time model to which an additional PIN does not need to be entered (at peak times etc.).

Table 12: Location table (defines which card groups get access to which room at which time)

Alias	Data type	Length	Description
ID	Number (int)	4	ID of the time model. All other tables refer to this data line via this number, if necessary.
Weekdays	Number (int)	7	Indicates the weekdays on which the following period of time should be applied to (form: 7 digits at most 1-7 e.g. 134567 = Monday, Wednesday till Sunday)
TimeStart	String (Time)	5	The start time for the period of time. (form: 24h HH:MM)
TimeEnd	String (Time)	5	The ending time for the period of time.

Table 13: Time table (grouping of single time zones (weekday from to) as a time model number)

Alias	Data type	Length	Description
Day	String (Date)	10	Date of the blocking day. (form: YYYY-MM-DD)
RefGroup	Number (int)	4	Indicates the authorization group to which the blocking day is applied. A zero defines a global validity for all groups.
RefTime	Number (int)	4	Indicates the assigned time model. (0 = not used) During this time access is granted. Thus, also "half holidays" like New Year's Eve can be realized.

Table 14: Holiday table (setting of blocking days like holidays or company holidays)

Alias	Data type	Length	Description
RefReader	Number (int)	4	Module (door module or master) on which is the digital input.
PortIn	Number (int)	1	Number of the digital input on the module.
RefAction	Number (int)	4	Reference to the action that should be carried out (e.g. switch relay).
RefTime	Number (int)	4	The time model which indicates when the digital input is checked. (0 = not used)

Table 15: Event table (assigning an action to a signal at the digital input)

Alias	Data type	Length	Description
ID	Number (int)	4	Action number, it can occur several times because of several actions that have to be worked through.
RefReader	Number (int)	4	Module (door module or master) on which an output(relay) is switched.
PortOut	Number (int)	1	Indicates the number of the output on the module.
Elapse	Number (int)	3	The duration of the switching of the relay (0 = permanently). Unit 200 ms
RefTime	Number (int)	4	The time model indicates when the output may be switched. (0 = not used)

Table 16: Action table (list of all workable actions in the access control system; an action group - all actions with the same action number - can switch several relays)

### 3.6.4 An example for a ZK system

On the basis of an example, it is demonstrated how an access control system is structured and configured.

The system consists of a RS485 bus via which a ZK-MasterIV communicates with a TS TMR33-TM and a TS TMR33-LTM. The TS TMR33-TM additionally communicates with a TS TMR33-L via a RS232 stub line.

Door 1 is controlled via the TS TMR33-TM. The cards of the access authorized persons are read at the TS TMR33-L and analysed by the ZK-MasterIV. If a person is authorized, the TS TMR33-TM receives a signal from the ZK-MasterIV and switches the open-collector for a given period of time in order to open door 1. Because the TS TMR33-L, which is an insecure are, is connected via a RS232 stub line, manipulation of the system can be ruled out.

Door 2 is controlled via the TS TMR33-LTM. The cards are read at this module and the data is transmitted to the ZK-MasterIV. In case of access authorization the TS TMR33-LTM receives a signal for switching the open-collector to which the door opener is connected.



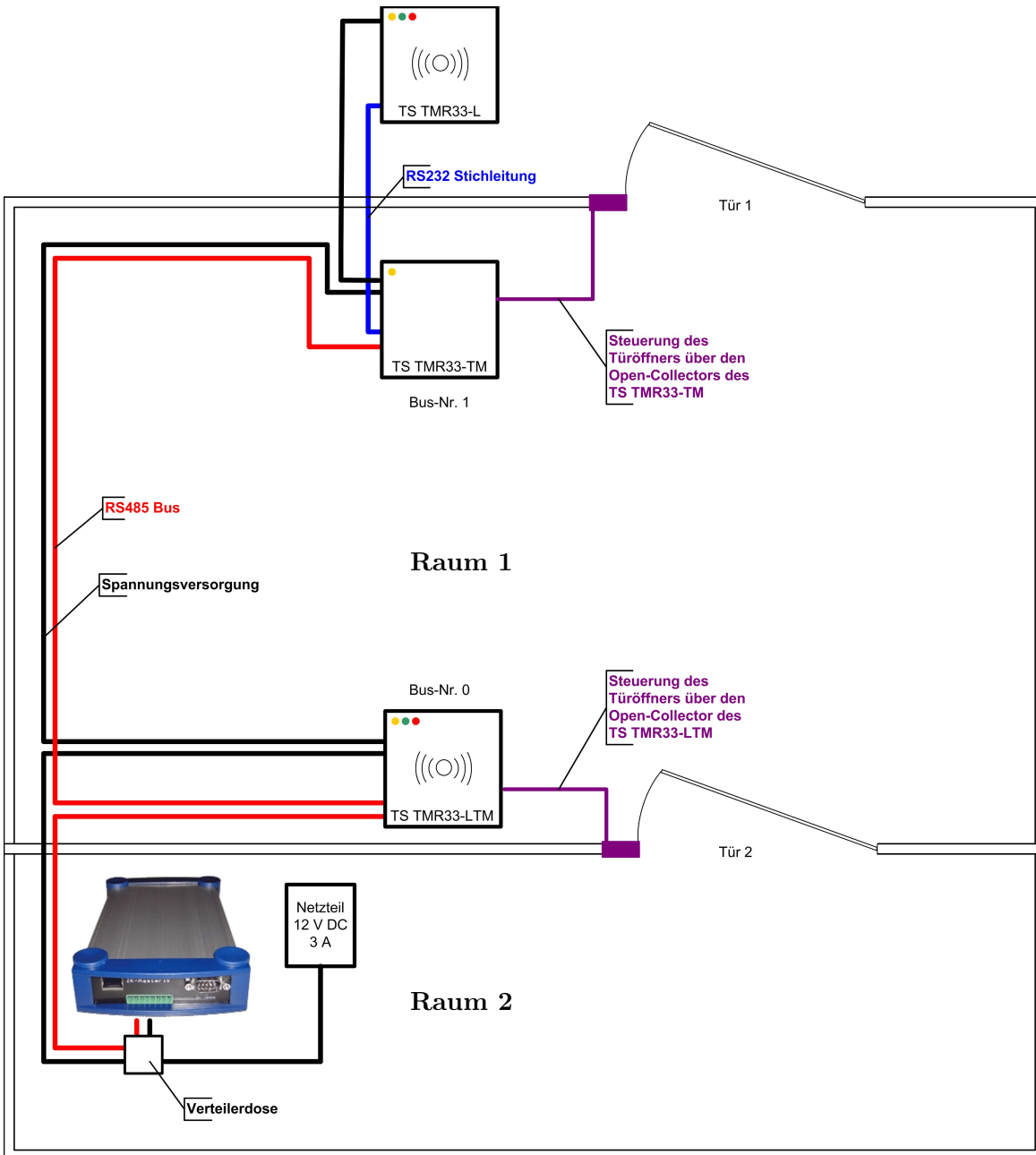
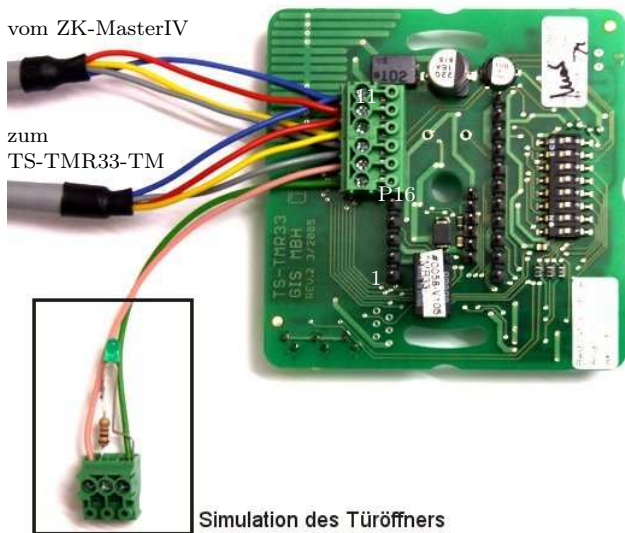


Figure 56: Schematic depiction of an example system



The power supply for the ZK-MasterIV and the access modules (TS TMR33) is established via the red wire (12 V DC) and the blue wire (GND). Note the information in chapter 3.2.1. The RS485 bus is connected via the yellow wire (data line A = +) and the grey wire (data line B = -). The 3 A power supply unit is connected to the cabling via an additional distribution box.

Figure 57: Connection of the ZK-MasterIV



The bus no. is set on 0 via the DIP switch on the door module with a reader (TS TMR33-LTM); the DIP switches 1 to 5 have to be at OFF. The DIP switch 7 always has to be at OFF. The module is not the last module in the RS485 bus. Therefore, the DIP switch 8 has to be at OFF. The power supply is established via PIN 10 (GND) and 11 (8 - 14 V DC) of the edge connector P16. The RS485 data channel A (+) is connected via PIN 8 and the data channel B (-) via PIN 9.

Figure 58: Connection and configuration of the TS TMR33-LTM for RS485

In this example, the door opener is connected via PIN 6 (open-collector -) and PIN 7 (open-collector +). The power is provided by the module. An additional voltage source is not necessary. However, you have to observe that the door opener has to work within a voltage range of 8 to 12 V DC and that the current consumption has not to exceed 100 mA. Otherwise, the door opener can also be switched via the relay. In that case, a voltage/ switching current of 42 V AC/0,5 A or 60 V DC/0,3 A at most is permissible.

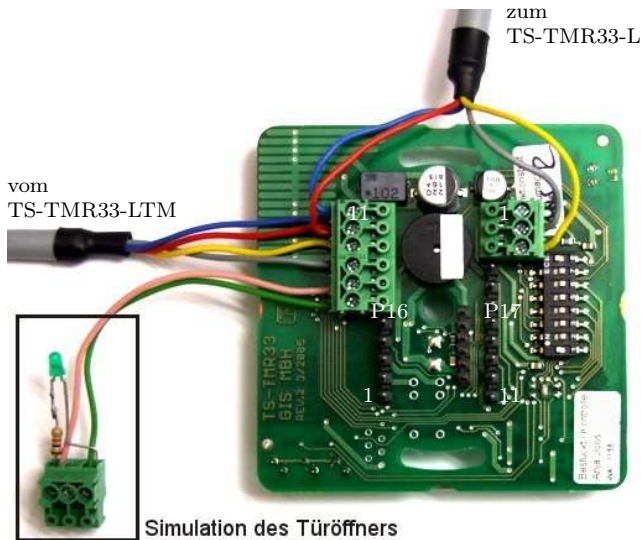


Figure 59: TS-TMR33-TM-RS485

The bus no. is set on 1 via the DIP switch on the door module without a reader (TS TMR33-TM); the DIP switch 1 has to be at ON, the DIP switches 2 to 5 have to be at OFF. The DIP switch 7 always has to be at OFF. Because the module is the last module in the RS485 bus, the bus with the DIP switch 8 has to be at ON. The power supply and the RS485 bus of the TS-TMR33-LTM is connected analogous to figure 58. The power supply for the external reader is established via PIN 10 and 11 of the edge connector P16.

RxD (grey) is connected via PIN 2 of the edge connector P17 in figure ... and TxD (yellow) is connected to PIN 3 of the RS232 stub line.



Figure 60: TS-TMR33-L-RS232-Stich

The communication with the reader (TS-TMR33-L) via a RS232 stub line is configured with the DIP switch 6 at ON. No bus number has to be set for the reader. The Dip switches 1 -5 are at OFF. The DIP switch 7 always has to be at OFF. The DIP switch 8 is also at OFF because no timing has to be turned on. The power supply of the module is established via PIN 10 and 11 of the edge connector P16. The RS485 data channel A is connected via PIN 3 and the data channel B via PIN 2 of the edge connector P17.

After setting up and wiring the system, the software configuration has to be done. All tables are mandatory. However, the tables holiday and event can be empty. The tables are displayed in the form of text files. You also can log comments within the text files for an easier maintenance of the system. You only have to start a comment line with a semicolon in the first column. They must not be configuration data within this comment line.

The Reader.txt (Reader table) has the following content:

```
; Reader list for the example access control system
; ID ZM TM RefLocation RefAction PinGeneral
1 1 320 0 0 0
2 1 000 1 1 0
3 1 010 2 0 0
4 1 011 2 2 0
```

The data record with the ID 1 stands for the ZK-MasterIV and receives number 1 as access master (ZM - Zutrittsmaster). The access master always receives the number 320 as TM value, that means it always receives the bus number 32. Because the ZK-MasterIV is not necessary for controlling a relay or door opener, you can enter 0 in the Location table for the reference to a data record. The same applies to the reference to the Action or as PinGeneral.

The data record with the ID 2 stands for the TS TMR33-LTM and is managed via the access master (ZM) 1. The module receives the number 000 as TM value; both numbers on the left stand for the bus no. 0 and the number on the right 0 marks the communication via RS485. At this place only 0 or 1 are permitted. This module is assigned to the room with the location-ID (RefLocation) 1. If an access is authorized, the action (RefAction) 1 shall be carried out. A PIN for an access without card (PinGeneral) is not used; therefore, the value at this place is 0.

The data record with the ID 3 stands for the TS TMR33-TM and is managed via the ZM 1. The module receives the number 010 as TM value. This value corresponds to the bus no. 1 with a communication via RS485. The module is assigned to the room with the location-ID (RefLocation) 1. Because the door module has no reader, it cannot set off an action in this example. As a note: it would be possible to set off an action via the digital or analogous inputs of the door module. It is also not possible to enter a PIN, thus, PinGeneral = 0.

The data record with the ID 4 stands for the TS TMR33-L and is also managed via the ZM 1. The module receives the number 011 as TM value. This value corresponds to the connection to the module with the bus no. 1 via RS232 via a stub line (data record 3). This module is assigned to the room with the location-ID (RefLocation) 2. If an access is authorized, the action (RefAction) 2 shall be carried out. A PIN for an access without card (PinGeneral) is not used; therefore, the value at this place is 0.

The Identification.txt (Identification table) has the following content:

```
; Identification list for the example access control system
; ID Group Pin Menace ActiveStart ActiveEnd ActiveGeneral
1111 1 1111 511 2005-01-01 2008-01-01 1
2222 2 2222 522 2005-01-01 2008-01-01 1
```

You can adjust the ID or the PIN and the menace code to your requirements, dependent on the card number you use. The time domain for ActiveStart and ActiveEnd can be set as well. If you do not have modules with a keyboard, you can also set the PIN and menace code on 0.

The Location.txt (Location table) has the following content:

```
; Location list for the example access control system
; ID RefGroup RefTime RefTimeNoPin
1 1 3 3
1 2 3 3
2 1 1 0
```

The first data record sets that the person group 1 gets access to room 1 for the time model 3 without needing to enter the additional PIN within the time model 3, because in this example the TS TMR33-L and the TS TMR33-TM has no keyboard. The second data record defines the same for the person group 2. The third data record sets, that only the person group 1 gets access to room 2 within the time model 1 and additionally has to enter the PIN defined in the Identification.

The Time.txt (Time table) has the following content:

```
; Time list for the example access control system
; ID Weekdays TimeStart TimeEnd
1 12345 07:00 13:00
2 12345 13:01 18:59
3 12345 07:00 18:59
```

In the time table the different time models are defined.

The Action.txt (Time table) has the following content:

```
; Action list for the example access control system
; ID RefRead PortOut Elapse RefTime
1 1 1 25 0
1 2 2 25 0
2 3 1 25 0
2 3 2 25 0
```

The first data record sets that the first internal relay (PortOut = 1) of the ZK-MasterIV (RefRead 1 = reference to the first data record of the reader table) is switched for the duration of 5 seconds. If you set Elapse on = you have to give a time model in which you define how long the relay should be switched. Otherwise, the switched relay permanently stays in this state. The second data record sets that the open-collector (PortOut = 2) is switched on the TS TMR33-LTM (reference to the second data record of the reader table) for the duration of 5 seconds. You can now deduce data record 4 and 5.

The tables Holiday and Event are not necessary for this example. With regard to the configuration of the holiday table it has to be mentioned that at first you set a holiday in the format YYYY-MM-DD. Next, you set the group for which this arrangement should be valid. If several groups are concerned, simply display the data record with the same date several times and change the group ID. In the third column of each data record you can additionally set a time model. By this way you can define half-holidays like Christmas Eve.

The data record 2006-12-24 1 1 in the holiday table with the time model 1 12345 07:00 13:00 means that on 24 Dec 2006 the person group 1 only gets access from 7 am to 1 pm (13:00).

With regard to the event table, the following things have to be mentioned: at first, you have to set the

module or the access master with a reference to the reader table on which the digital input is to be supervised. The second value gives the number of the digital input. The third value is a reference to the action table; this action is carried out if the level of the digital input changes. The fourth and last value is a reference to the time table for setting the time model which is valid for the execution of the action.

Even if you do not need the holiday and event table, they have to be generated as \*.txt files (empty) and be transmitted to the device together with the other files.

If you have paid attention to the construction and configuration instructions and their hints, you can transmit the lists (tables or text files) to the ZK-MasterIV with a standard setup for the access control and test them.

### 3.7 Timing of the digital exits for the MasterIV device series

It is possible to time the digital outputs of the MasterIV device series via tables. Thus, for example a turn down of the heating system at night, a buzzer control and much more can be realized.



**Caution:**

In order to use the timing of the digital exits, the firmware version 04.01.01.17 (or higher) has to be installed on the terminal.

The following tables have to be configured:

- ▶ Action
- ▶ Reader
- ▶ Time

**Description:**

Each action that should be activated has to be entered in the table Action. The table Action refers to the tables Reader and Time. In the table Reader the module is left on which the relay or the Open Collector is to be switched. The reference to the table Time indicates when the switch shall be done. If start and stop time are entered, the relay is **switched on** when exceeding the start time and **switched off** when exceeding the stop time. The entry of the duration **Elapse** in the table Action is ignored. If the relay should only be activated for a few seconds, e.g. for a buzzer control, the stop time has to be set on "00 : 00". If the start time is exceeded, the respective exit will be switched for X seconds (*RefTime* in Action table). The entry **Elapse** in the table Action now indicates the on-time.

**Example:**

- ▶ A buzzer is to be activated for **3** seconds from Monday to Friday at **10.00** am and 4 pm **16.00**. The buzzer is controlled by the internal relay of the ZK-MasterIV.
- ▶ The heating system is to be turned on the "day mode" at **07.00** am and on the "night mode" at 7 pm **19.00** on all weekdays. The corresponding relay is at the door module with the bus number **2**.

**Reader.txt**

```
; ID ZM TM RefLocation RefAction PinGeneral
1 1 320 0 0 0
2 1 020 0 0 0
```

**Time.txt**

```
; ID Weekdays TimeStart TimeEnd
3 12345 10:00 00:00
4 12345 16:00 00:00
5 1234567 07:00 19:00
```

**Action.txt**

```
; ID RefRead PortOut Elapse RefTime
6 1 1 15 3
7 1 1 15 4
8 2 1 0 5
```

### 3.8 Access control II with PHG modules

The following hardware is available to set up an access control with PHG modules. The devices can be combined in different ways according to their hardware requirements.



#### ZK-MasterIV

Because the ZK-MasterIV is only used for the access control, door and remote monitoring, you can supervise up to 16 doors with one device and control 18 doors at most.



#### VOXIO

Unterputz: 81 x 81 x 11 mm (BxHxT)

Aufputz: 81 x 81 x 40 mm (BxHxT)

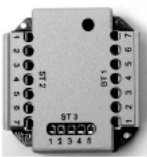
The VOXIO can be used with Legic or Mifare. It is available for in-wall or on-wall mounting with or without keyboard. Each reader has a sabotage recognition, three lamps for visualising the state and a buzzer for the acoustic signalling.



#### RELINO

50 x 50 x 43 mm (BxHxT)

The RELINO reader can be used with Legic or Mifare. It is available for in-wall mounting. Each reader has three luminous fields for visualizing the state and a buzzer for acoustic signalling.



#### I/O-Box

51 x 48 x 22 mm (LxBxH)

The I/O-Box as equipment for the RFID-wall reader or RELINO reader has two digital inputs and two digital outputs. The I<sup>2</sup>C bus is used as interface.



### 3.8.1 Connection

In order to connect the PHG modules please note the PHG documentation on the Datafox CD:

..\Datafox-Geräte\Datafox-Zutritt-Module\PHG \*.pdf

In the PHG documents for the single modules the pin assignment and configuration via the DIP switches are described. In order to carry out an access control with the ZK-MasterIV the option "access" has to be integrated (Datafox Art. no. 105201). The following figure shows the possible connections of PHG devices to a ZK-MasterIV for an access control.

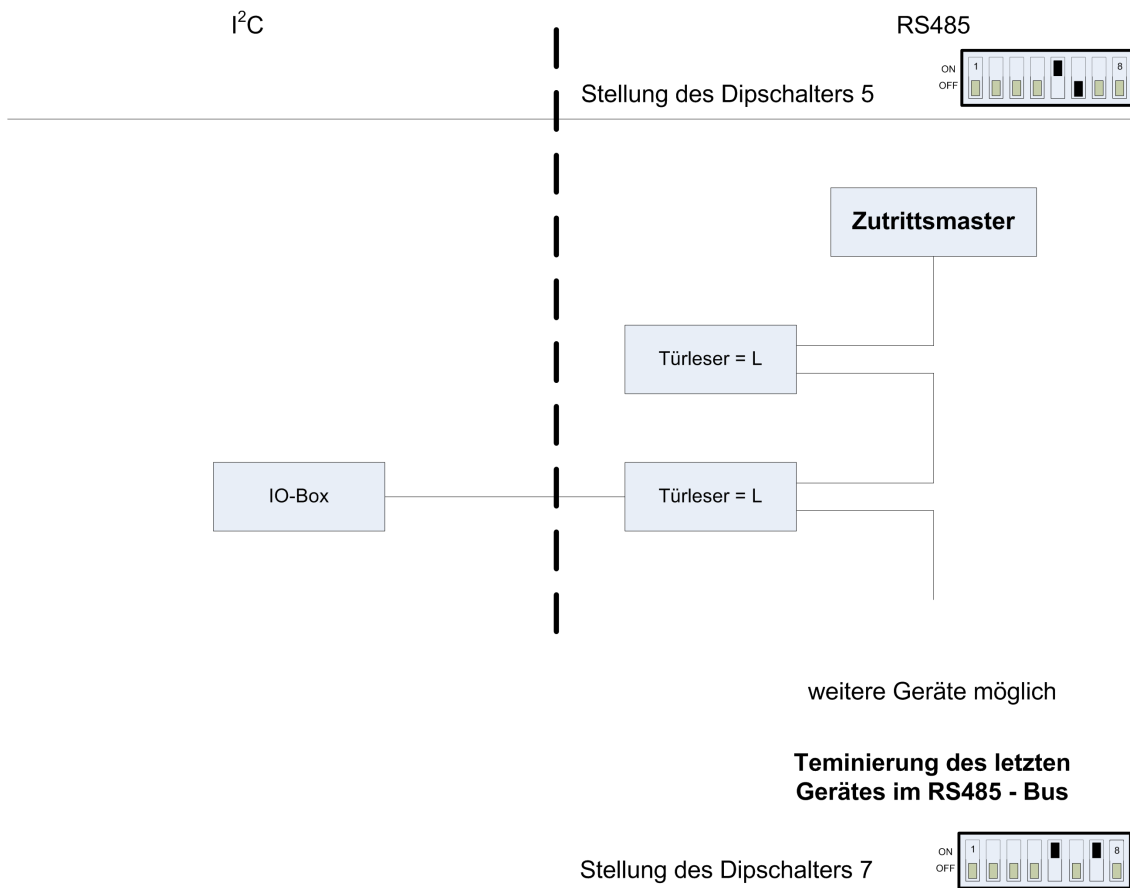


Figure 61: Connection of the access control II

The bus number of the module is set via the DIP switches 1 - 4. The DIP switch 5 always has to be at "ON". The DIP switches 6 and 8 always have to be at "OFF". With the DIP switch 7 = "ON" the RS485 bus is terminated at the last module, otherwise always "OFF".

If additionally a door-opener is to be controlled via a relay, the IO-box has to be used. With the IO-box two digital exits as relays are available.

### 3.8.2 Configuration

The access modules of PHG with phg-crypt-protocol use an encryption in accordance with the Rijndael / AES-128 standard (AES - Advanced Encryption Standard). The code is set in the setup under access after selecting the access series. The 1685 protocol of PHG is not supported by Datafox.

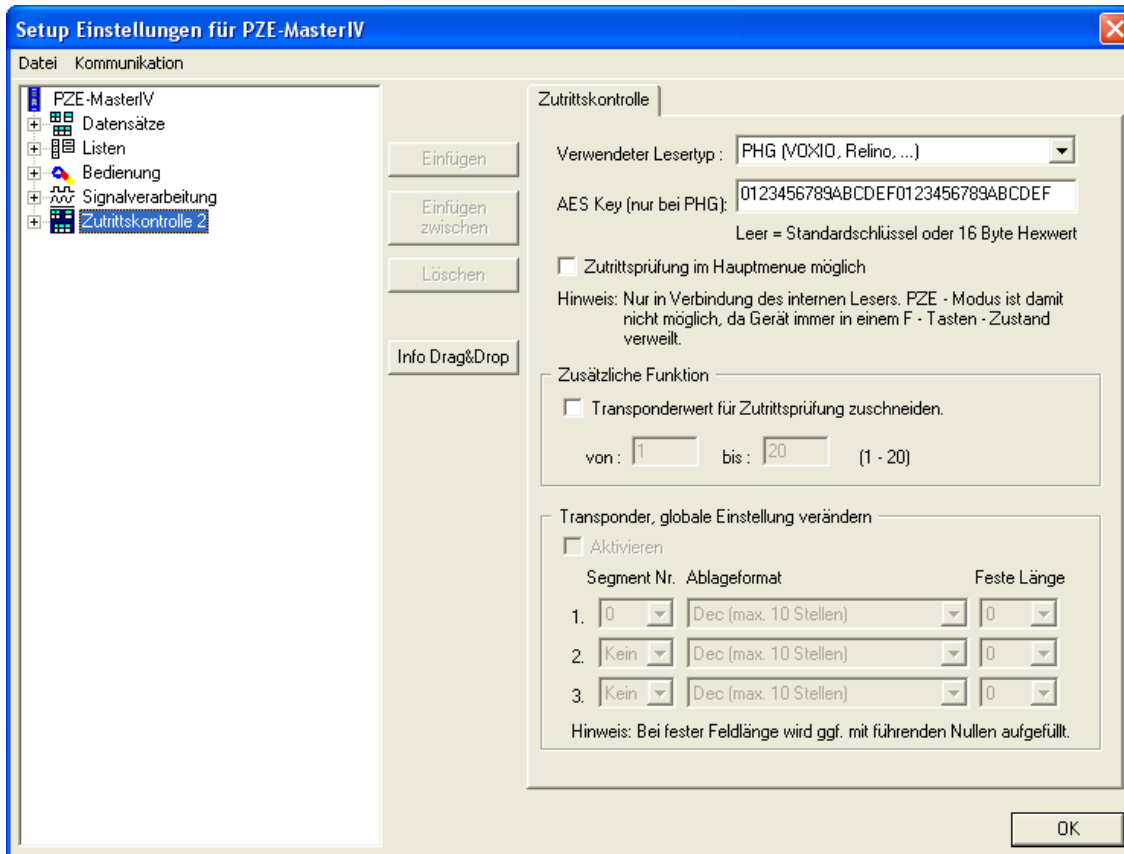


Figure 62: Communication key for the PHG-crypt protocol

The modules always work with encryption. If no code is entered, a not published standard code is used; otherwise, the entered user code is used. Please use all the 16 byte of the code.

All door modules that are compiled in the reader table have to be available in the RS485 network in order to guarantee that the code can be changed in all modules, if a new setup with a different code is loaded. If a door module from the list is missing in the bus, no change of the code takes place. The old setup with the old code has to be reloaded; otherwise, after rebooting the device it is not possible to communicate with the door modules until the right code is used again.

If a defective reader is replaced by a new reader that has not been used yet, the firmware recognizes this automatically at the start and sets up the encryption. The reader can also be changed during operation, the firmware automatically integrates it.

If you have forgotten the user code for a door module, there is no possibility to activate the readers. The reset of the forgotten key at the reader can only be done by PHG.

### 3.9 Status message of the access control

For the admission control following state messages are defined. The decimal values of the state message can be saved to every data record.

Display	Assigned status message
0	Module recognised, everything is okay
3	Module not defined in the list but found in the bus
4	Module from the list not found in the bus
5	Module wrong coding password
6	Module wrong login password
7	Module wrong reader type (Mifare, Legic, Unique, etc.)
8	Module error while configuring the module
9	Module neither found in the list nor in the bus (is not used)
10	The communication key for the PHG-Crypt-protocol has been changed
11	The communication key for the PHG-Crypt-protocol has not been changed

Table 17: Initialization / Communication

Display	Assigned status message
20	Access granted for this card number
21	Card number not contained in the identification list
22	Card number blocked
23	Time of validity of card number expired
24	Room not contained in the location list
25	No access during this time
26	Awaiting PIN entry (green LED flashes)
27	Entered PIN is invalid
28	PIN with menace code was entered
29	Entered PIN is OK
30	Entered master PIN is OK
31	Time-out for PIN entry
32	Card number with general authorization
34	Card number in the online mode read
35	PIN in the online mode read
100	Access control deactivated in the setup
101	At the moment the access control cannot be called up (busy)
102	Access control needs the lists
103	Incorrect bus type (Datafox, PHG, etc.)

Table 18: Access control

Display	Assigned status message
40	Digital output 1 is low (off)
41	Put digital output 1 on high (on)
42	Digital output 1 is trigger (on for given period of time)
43	Digital output 2 is low (off)
44	Put digital output 2 on high (on)
45	Digital output 2 is trigger (on for given period of time)

Table 19: Digital Output

Display	Assigned status message	
	GIS	PHG
60	Digital input 1 is low	IO-Box closed
61	Digital input 1 is high	IO-Box open
62	Digital input 2 is low	IO-Box closed
63	Digital input 2 is high	IO-Box open
64	Digital input 3 is low	sabotage supervision -> communication channel OK
65	Digital input 3 is high	sabotage supervision -> communication channel interrupted
66	Digital input 3 was interrupted	PHG not used
67	Digital input 3 was short-circuited	PHG not used
70	not used	Digital input 1 reader low
71	not used	Digital input 1 reader high
72	not used	Digital input 2 reader low
73	not used	Digital input 2 reader high
74	not used	Alarm control panel -> state of device OK
75	not used	Alarm control panel -> device manipulated

Table 20: Digital Input

## 4 DatafoxStudioIV - General operation



### Note:

The dialogues can differ from the presentations in this manual, dependent on the version of the DatafoxStudioIV. This also applies to differences in functionality.

### 4.1 Installation

The DatafoxStudioIV is required for setting up and changing the device setup. The setup and communication program just consist of the files DatafoxStudioIV.exe and DFComDLL.dll. A real installation is not necessary. Just copy the files into the desired directory and create a link to DatafoxStudioIV.exe in the program menu or at the desktop.

#### System requirements

- ▶ PC with Microsoft Windows 95/98/NT/2000/ME/XP
- ▶ 64 MB RAM
- ▶ minimum 2 MB HD memory

#### Use



### Caution:

If there are different versions of the DFComDLL.dll on the PC where the program DatafoxStudioIV is run, it can lead to malfunctions, because possibly a wrong version of the DLL is loaded by the program. Therefore, always pay attention to the software version and compatibility (see chapter 2.1).

#### User interface

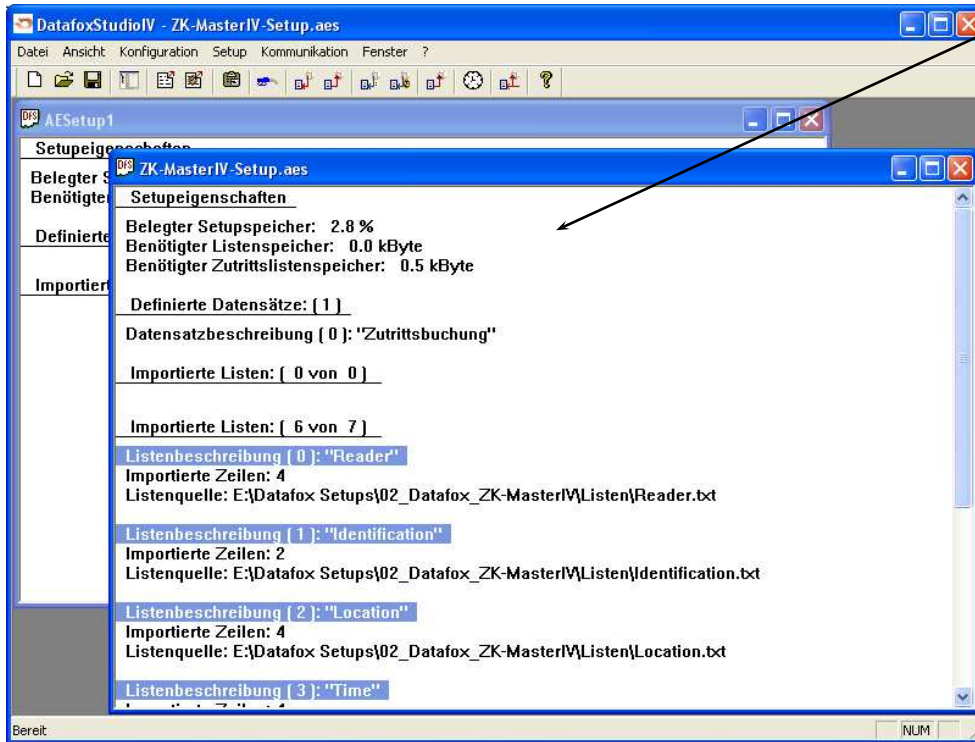
##### Description of the main menu items

File:	Open, save, create setup file
View:	Hide and unhide status bar and toolbar
Setup:	Basic settings like edit setup, import lists, set data storage, load firmware and device maintenance via modem connection
Communication:	Setting of the communication, commands for a communication between the PC and the terminal
Window:	Set the order of the windows
?	Information about the program and version requirements for the firmware and DF-ComDLL.dll

The single functions are explained in detail in the following chapters.

### 4.2 Operation of the DatafoxStudioIV

All functions you need about the setup are available via the menu of the DatafoxStudioIV. The most important functions can additionally be called up via the toolbar.




**Client-Window**

The edition, e.g. writing setup, etc., always refers to the current marked window. The file name of the setup file is visible in the title bar.

Figure 63: DatafoxStudioIV User interface

As long as the setup-mask-dialogue is opened you have no access to other functions of the DatafoxStudioIV. Only if the dialogue is closed, you can call up and carry out other functions from the studio for the setup that is chosen currently.



**Note:**

Please take into consideration that, if several setups have been opened in the main window of the DatafoxStudioIV, the changes only refer to the currently chosen setup. This means the setup window which is not covered by another window.

### 4.3 Menu Datei

Under the menu item < *Datei* > are several standard functions that you know from other office applications and that are not examined further. Such functions are for example < *Speichern* > for saving changes.

#### 4.3.1 Creating a new setup file

You can create a new setup file via < *Datei* => *Neu* >. A new client window will be opened in the DatafoxStudioIV. After creating a setup file you should save it under the name of your choice. After successfully saving the setup file the new file name will be displayed in the title bar of the client window. With that, the creating of a new setup file is finished. The setup now can be edited at will.

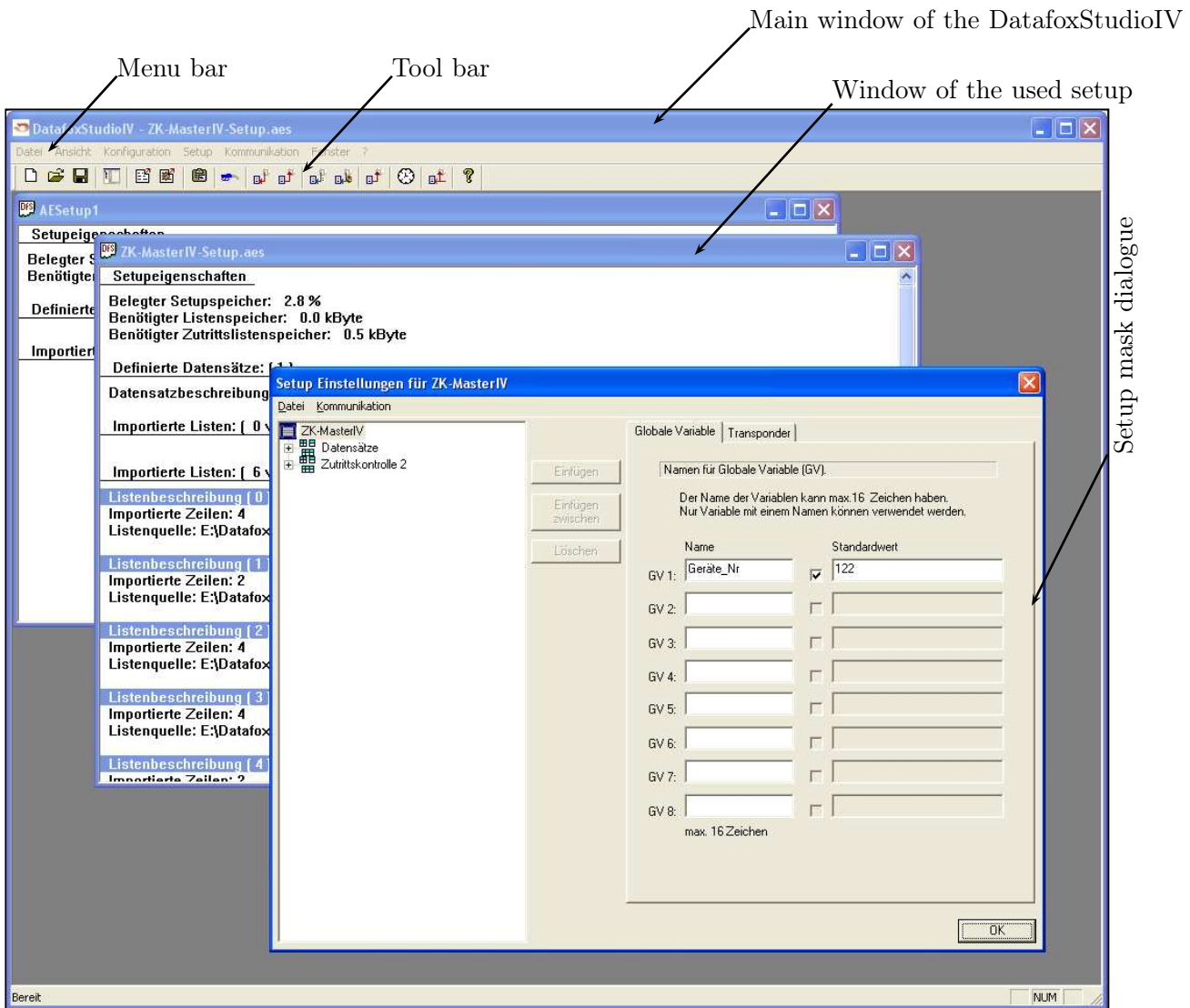


Figure 64: User interface of the DatafoxStudioIV

### 4.3.2 Open setup file

In order to open an already created setup file with the DatafoxStudioIV, click on < *Datei* => "Of fnen" > in the menu and select the directory that contains the file. Open the file with a double click on it.

**! Caution:** You should note that if you open a setup file that was created with a previous version of the DatafoxStudioIV, the file is converted into the new setup format by the DatafoxStudioIV. Then, it is not possible any longer to open this converted setup file with the previous program version. The DatafoxStudioIV back-ups the setup file before converting it. The back-up copy has the file extension (\*.bak). By renaming the file extension (.aes) you can open and edit it with a previous program version (AESetup).

## 4.4 Menu Setup

### 4.4.1 Edit

Via the menu item < *Setup* => *Editieren* > you reach the domain of the DatafoxStudioIV where you can edit a setup. You can find a more detailed description of the procedure in chapter 5.



**Note:**

By double clicking on the white surface of the window, this menu order is carried out as well.

### 4.4.2 Import access control lists

The access control lists are defined in the setup with a fixed name and structure.



You can import all necessary access control lists into the setup program via the menu item < *Setup* => *Zutrittskontrolllisten Listen importieren* >. Select the lists as shown in the figure opposite and open them. You can select several files at the same time by pressing and holding the Ctrl key.

Figure 65: File selection dialogue for the import of access control lists



#### 4.4.3 Configure data storage

Under the menu item < Setup => *Datenablage konfigurieren* > a dialogue opens where you can set how the read out data records should be saved.



Figure 66: Configuration of the data storage

You can define if an existing file should be overwritten or if the data shall be added to the file.

Furthermore, you can set the output format and define if and how field names should be used in the data files in order to be able to identify the field values more easily.



**Caution:**

If you read out data from several terminals and want to unite them into a single file, you necessarily have to activate the option "Add data to file" in order to avoid data loss. Otherwise, only the data of the terminal that was read out last are preserved.

4.4.4 Load firmware

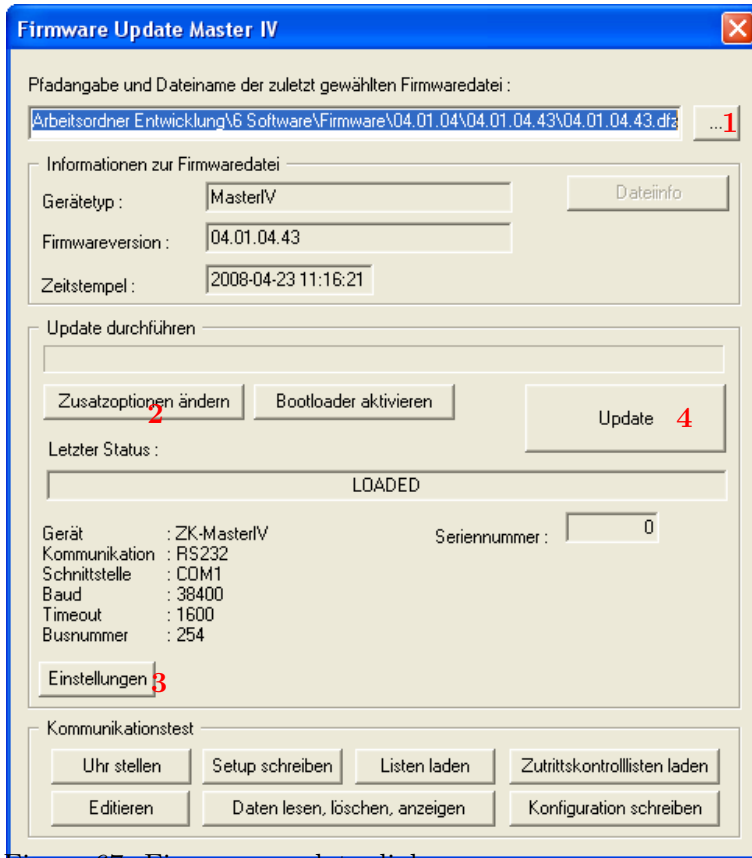


Figure 67: Firmware update dialogue

You can make all necessary settings for a firmware update via the menu item < Setup => *Firmware laden* >.

You can select a \*.zip archive which contains the firmware file (\*.hex) for the ZK-MasterIV via the button (1).

Via the button < *Zusatzoptionen ändern* > (2) you can select the access series (TS/ PHG) you use. It is important that this is done **before** the firmware update, otherwise the wrong firmware (wrong access series) could be installed.

Before transmitting the < *Einstellungen* > (3) for the communication (kind of communication, timeout etc.) should be checked. If all settings are correct, the update can be started via the button < *Update* > (4).

!

**Caution:**

Please note at all costs the information under software versions and compatibility as well as firmware update/ downgrade in the chapters 2.2.1 and 2.2.2.

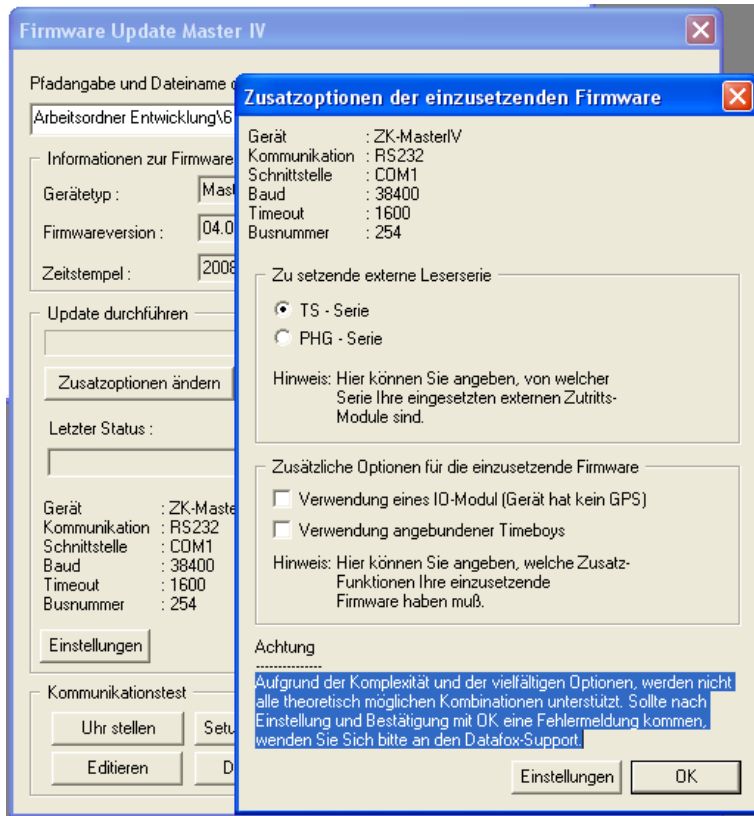


Figure 68: Additional options

With the Additional options you can define which additional functions have to be provided by the firmware.

This is especially important for the firmware updates from version < 04.01.04.32. In this case at first a firmware update with the version >= 04.01.04.32 has to be done. Only then the terminal can set the additional options.

Now set the additional options and apply them to the terminal by pressing OK. It is very important that now you do again a firmware update.

Only now, with the information from the terminal, the DatafoxStudioIV can select the appropriate firmware from the device file archive via the additional options.

#### 4.4.5 Device maintenance via modem connection

It often happens that a ZK-MasterIV is autarkically installed as data entry terminal at a machine or plant. In this case it would be very time-consuming to do a firmware update with direct connection to a PC. Therefore, it is possible to transmit data to the device or read them from the device via a modem connection.

All settings to take here, except for the PIN and phone number, refer to the configuration of the modem at you PC. That means, the external modem at the terminal has already to be configured for such a connection.

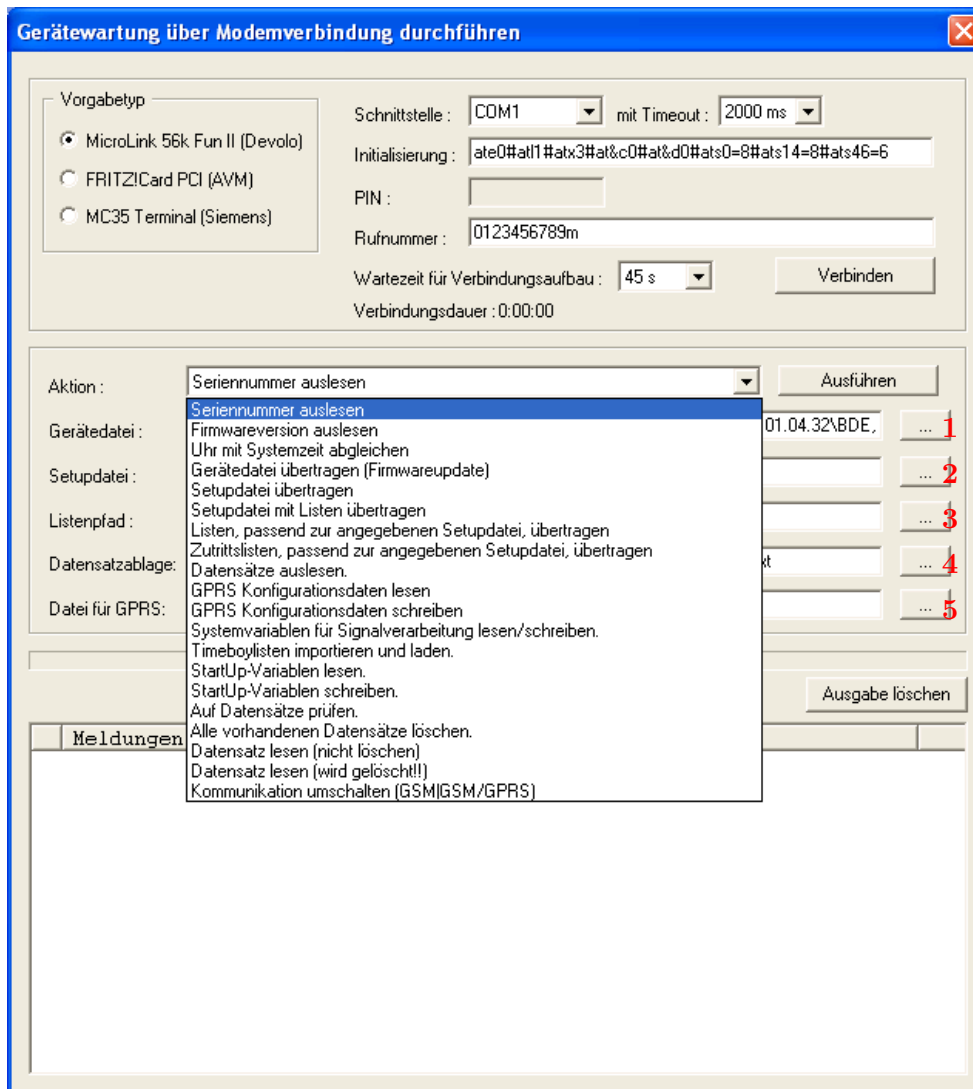


Figure 69: Device maintenance via modem connection

#### 4.4.5.1 Functions for device maintenance

- ▶ Read out serial number
- ▶ Read out firmware version
- ▶ Compare clock with system time
- ▶ Transmit device file (firmware update) - Via the button **1** in figure 69 a dialogue opens where you can select the device file with the extension ".hex". When you have marked the file, you can take it over via the button "Open".
- ▶ Transmit setup file - Via the button **2** in figure 69 a dialogue opens where you can select the setup file with the extension ".aes". When you have marked the file, you can take it over via the button "Open".
- ▶ Transmit setup file with lists - Via the button **3** in figure 69 a dialogue opens where you can define the folder (path) that contains the list files.
- ▶ Transmit lists matching to the given setup file - Only the list data of the button (**3**) are transmitted here.
- ▶ Transmit access lists matching to the given setup file - Here the access lists have to be assigned to the button (**3**)

- ▶ read out data records - Via this function you can read out data records from the ZK-MasterIV. Via the button **4** in figure **69** a dialogue opens where you can define the folder (path) in which you want to save the data records.
- ▶ Read GPRS configuration data - Via the button **(5)** a dialogue opens where you can define the GPRS.ini. Just create a new file, name it GPRS.ini and select it. Now, the current GPRS configuration is read from the device and written into the \*.ini file.
- ▶ Write GPRS configuration data - Select the configuration file (GPRS.ini) that contains the desired settings via the button **(5)**.
- ▶ Read/ write system variables for signal processing - A selection dialogue opens where you can select the desired system variables of the digital inputs and then read or write them. See chapter **4.5.8**.
- ▶ Import and load Timeboy lists - The dialogue "Import and transmit data of the lists of the Timeboy" opens. See chapter **4.5.3**.
- ▶ Read StartUp variables - Via this function you can read out the StartUp variables.
- ▶ Write StartUp variables - Via this function you can write StartUp variables.
- ▶ Checking for data records - It is examined whether there are data records in the device.
- ▶ Delete all existing data records - Deletes all data records from the device. This is absolutely necessary before you can install a new firmware or setup.
- ▶ Read data record (not delete) - reads a selected data record without deleting it
- ▶ Read data record (is deleted!) - reads a selected data record and then deletes it
- ▶ Switch over communication (GSM, GSM/GPRS)



**Note:**

In order to carry out the functions "Transmit device file" and "Transmit setup file", no data records must be on the device. In this case you first have to read out all data from the device (see chapter **4.5.4**).

#### 4.4.6 Edit text data of the firmware

From version 04.01.06. x you can edit the text data of the device firmware about DatafoxStudioIV. Open the edit dialogue about the menu < Setup => *Textdaten der Firmware bearbeiten* >. Open now an device file archive \*.dfz. The Defaulttexte of the firmware with a description are indicated.

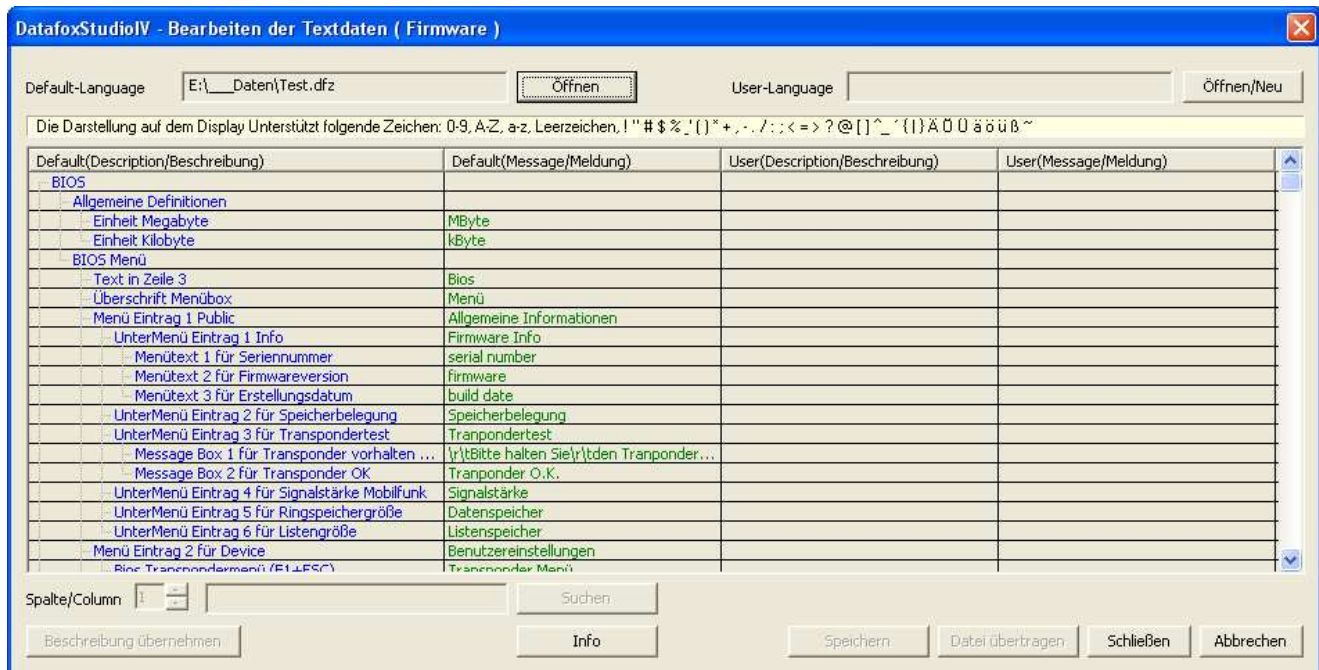


Figure 70: Default Text-Datendatei Öffnen

Open or generated now a new linguistic file for the firmware with the ending \*.dfi. If you have generated a new file, the right side of the list is empty.

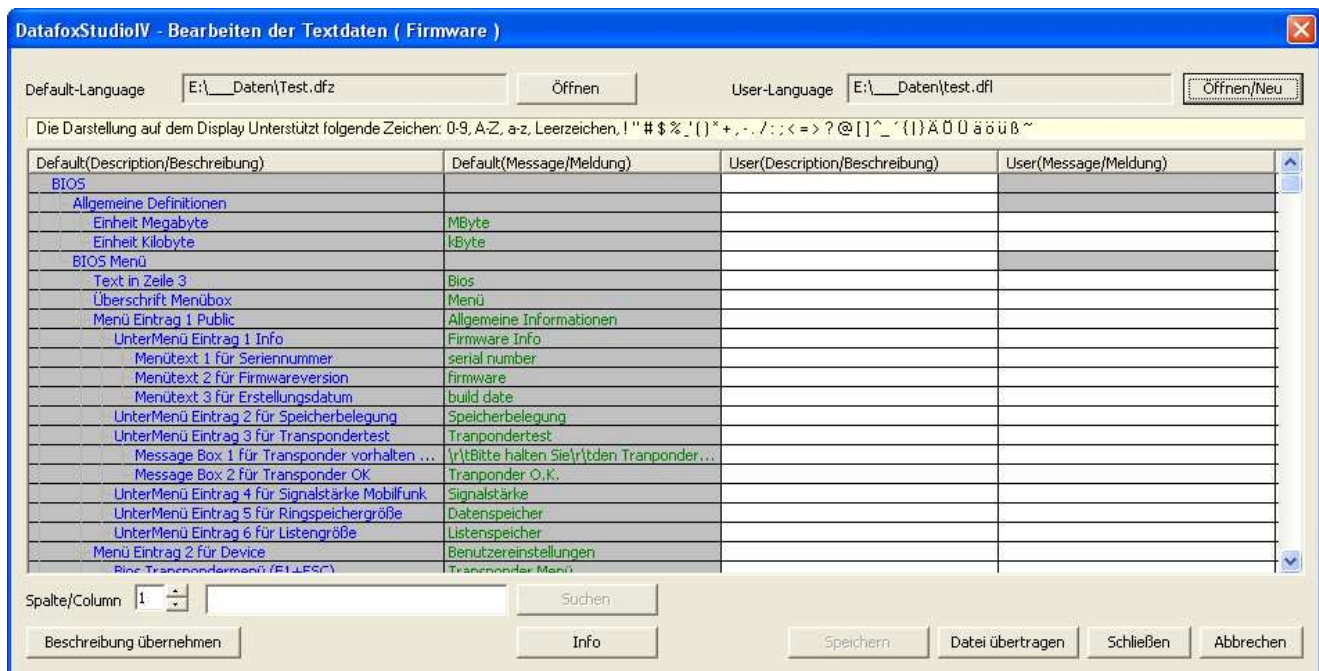


Figure 71: User Text-Datendatei Erstellen bzw. Öffnen

Innerhalb der Liste arbeiten Sie nur mit einfachen Mausklicks, KEINE Doppelklicks. Selectieren Sie mit einem einfachen Klick eine Zeile aus der Liste.

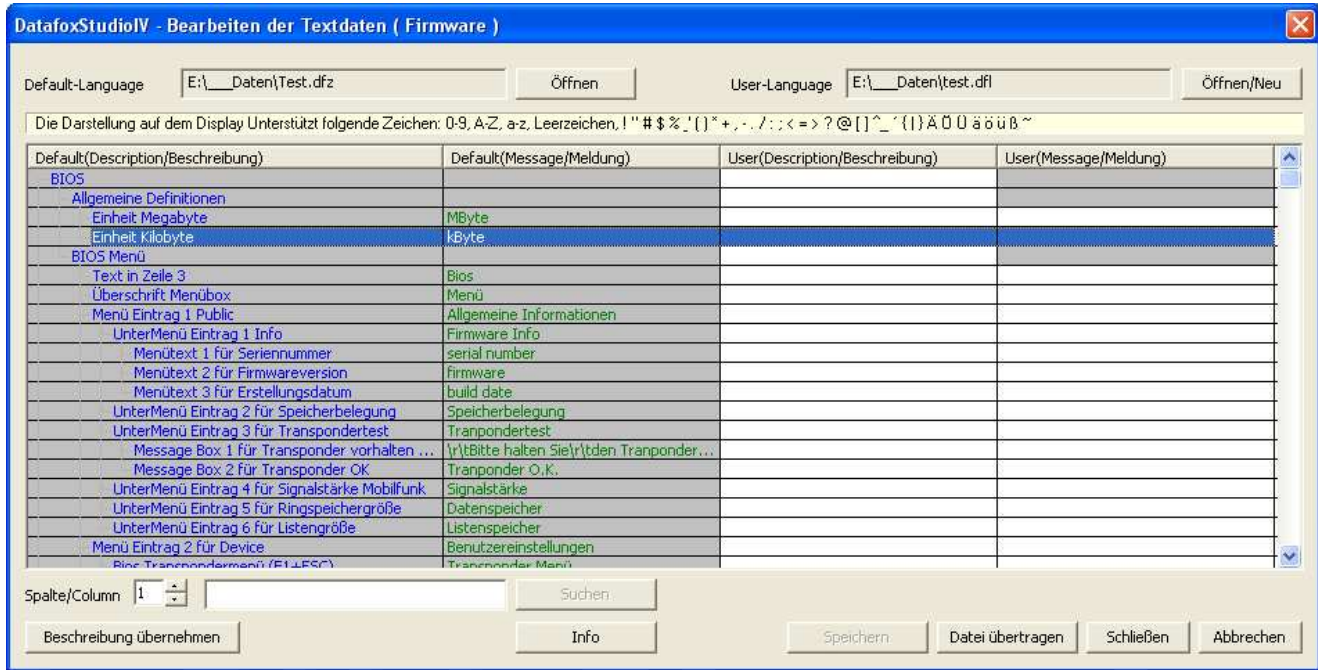


Figure 72: Zeile auswählen

With the next single click in the column of user(description/...) or user(message/...) you put the cursor in this field.

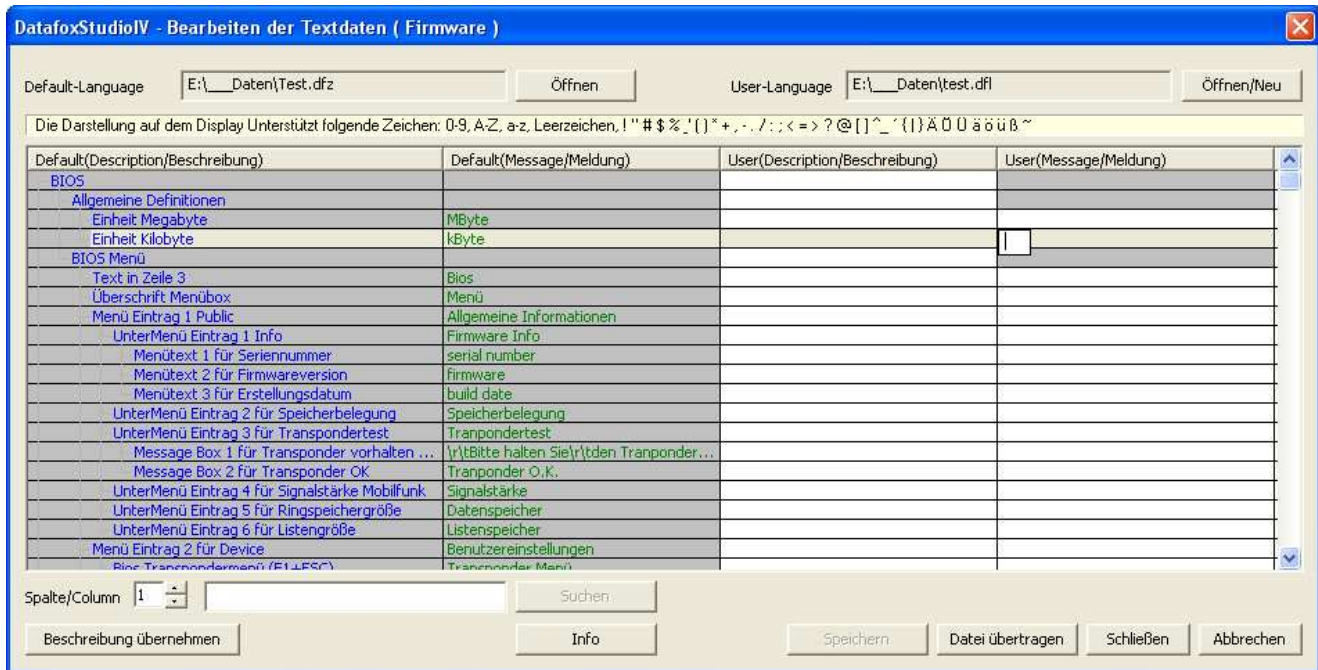


Figure 73: Zelle zum Bearbeiten auswählen

Now you can edit the text.

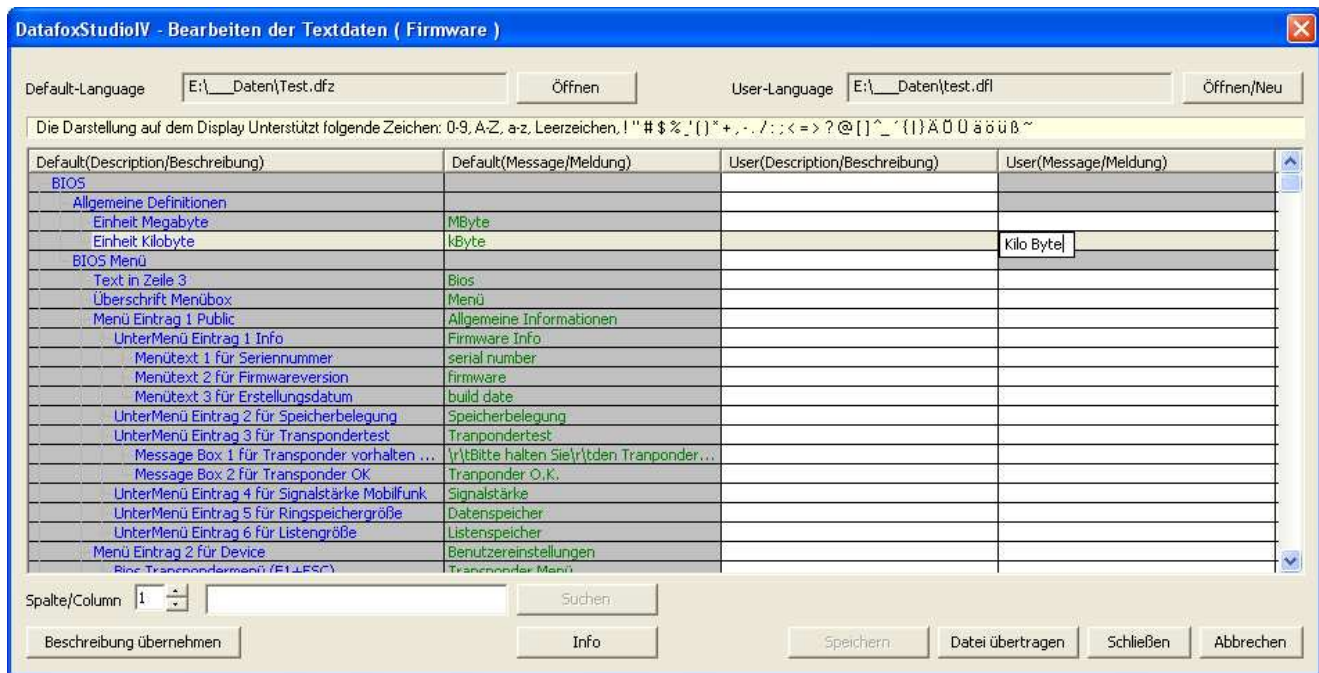


Figure 74: Textdaten eingeben bzw. bearbeiten

If you conclude the input, the description from the column default(description/...) is taken over.

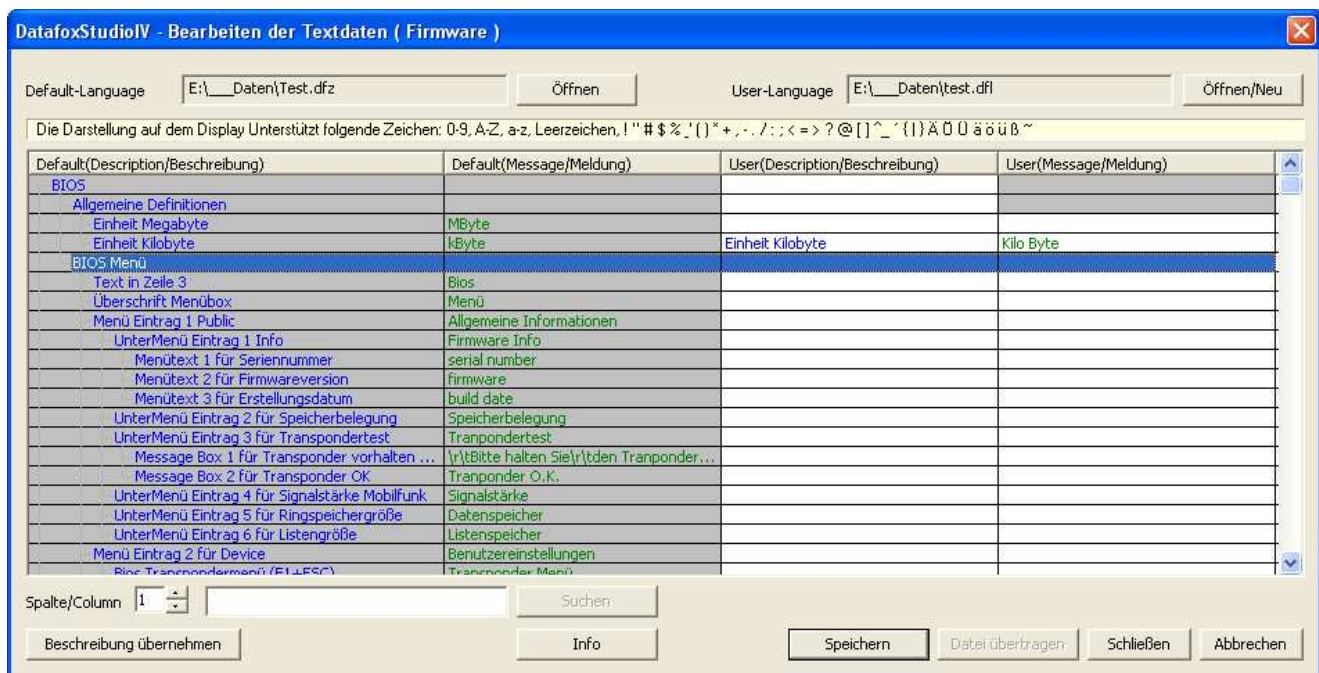


Figure 75: Änderungen übernehmen

You can change this text now in the column user(description/...). To transfer user to text data, they store all changes.

It is available to you a full text search. Give the text and choose the column which you would like to search for the text.



## 4.5 Menu Communication



### Note:

You can and should check all displayed communication parameters at each dialogue that opens with one of the following function calls, and adjust them via the button Settings if necessary.

### 4.5.1 Write / read setup

When the setup is finished, back-up it on disk via *< Datei => Speichern unter >*. For transmitting the setup you have to set the communication parameter for the device in question via *< Kommunikation => Einstellungen >*.



### Caution:

Always check the communication parameter before transmitting the setup. This is especially important when several devices are managed via the DatafoxStudioIV. Pay particularly attention to the IP address of the device to which you want transmit the setup.



Figure 76: Transmitting setup data

The device is only ready for operation with a completely transmitted setup. If the transmission is aborted early, the device cannot be put into operation. In this case, a possibly existing disturbance source has to be eliminated and the transmission must be repeated.

Likewise, a setup can be read out from the device in order to change it or to configure a second device with the same setup. Open the corresponding dialogue via *< Kommunikation => Setup lesen >*, give a file name for the setup and check the communication settings. With OK you confirm all entries and the setup is read out from the device.

### 4.5.2 Load lists/ access control lists

For the access control no normal list definitions can be created in the setup. The list definitions that are necessary for the access control are permanently logged in the setup. For this reason only access control lists can be imported.

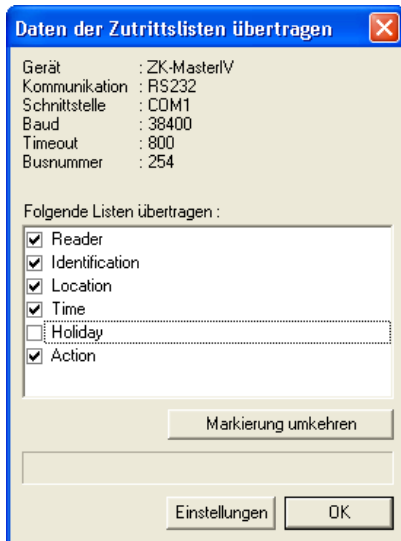


Figure 77: Load lists

The loading of the lists / access control lists is done via the function `< Kommunikation => Listen laden >` or for the access control via `< Kommunikation => Zutrittskontrolllisten laden >`. This functions are also available in the DLL and can be used via own applications.

If devices are activated via the DLL, the lists can be directly transmitted from an application without previously creating an ASCII file.

### 4.5.3 Import and load Timeboy lists

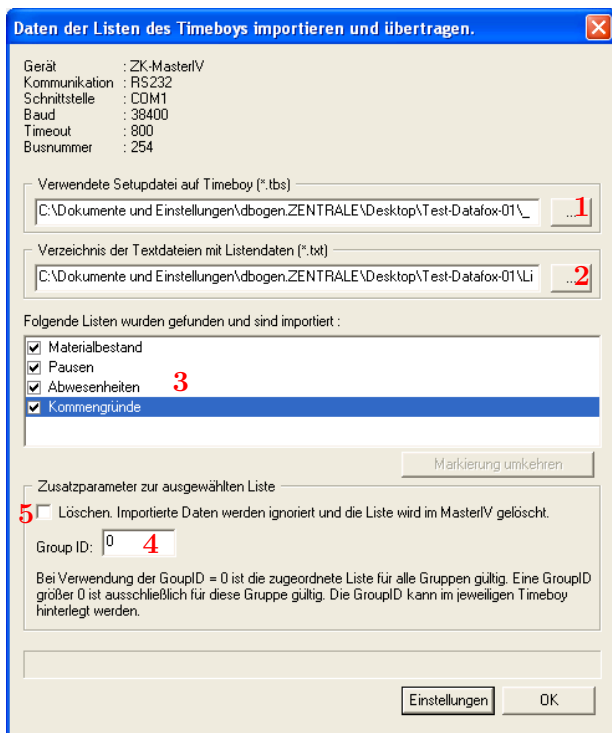


Figure 78: Import and load Timeboy lists

You can start the dialogue for importing Timeboy lists via the function `< Kommunikation => Timeboylisten importieren und laden >`. Here, at first you select the path to the desired Timeboy setup (1) and then the path to the Timeboy lists (2). The lists whose information matches the list description of the Timeboy setup are displayed now (3). You can define the Group ID (4) via the additional parameters and thus assign the special lists e.g. for certain fields of activities. The Group ID is logged on the Timeboy. Additionally, you can delete lists from the ZK-MasterIV (5).

This functions are also available in the DLL and can be used via own applications.

#### 4.5.4 Read, delete, display data

The setup program offers simple functions for reading out and deleting data from the device. Only ASCII files can be created. For different output formats the use of the communication DLL or Datafox-Talk is advisable. Please not chapter 2.3.2.

The respective formats and options for the filing of data in the ASCII file are set via *< Setup => Dateiablage konfigurieren >*, as described in chapter 4.4.3.



#### Caution:

In a network the option "Add data to file" (if this file already exists) has to be activated. Otherwise, at the download the data are overwritten by the following devices and only the data from the last device are available.

##### 4.5.4.1 Read data and delete them

You can read out the data records from the device via the menu *< Kommunikation => Daten lesen, löschen >*. The reading out of the data records is done separately.

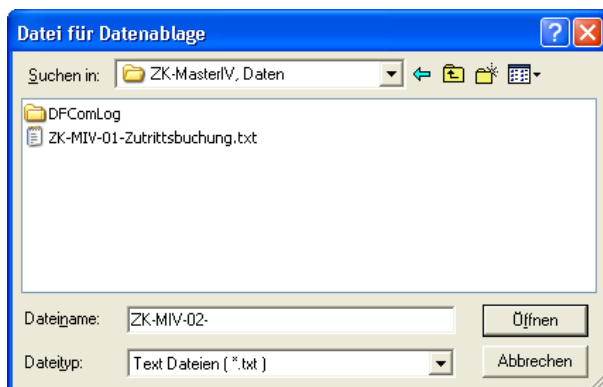


Figure 79: Selection/ setting of the file repository

After the function call

*< Daten lesen, löschen >*, a file name for saving the data records has to be given. If more than one data record description is defined in the setup for the access control lists, only one prefix has to be given for the device code. The names of the data record descriptions are used as file extension. For each data record description of the used setup, an own text file is created for the existing data records.

#### 4.5.5 Set time

Via the function *< Kommunikation => Uhrstellen >* you can compare the time of the device with the system time of the PC from which this function is called.

#### 4.5.6 Read serial number

With the function *< Kommunikation => Seriennummer lesen >* you can read out the number of a device. It is displayed via a separate dialogue.

#### 4.5.7 Read global variables



Figure 80: Values of the read variables

Via the function "Read global variable" you can check which value has a global variable in the device.

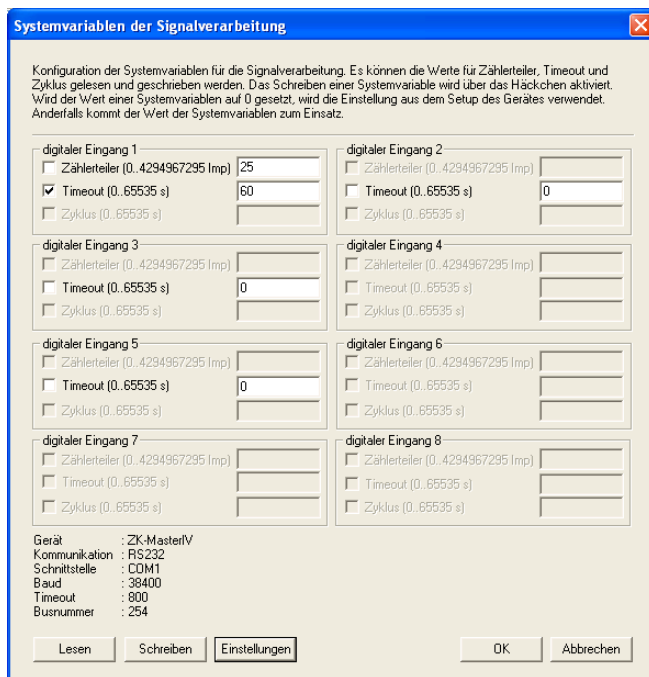


Figure 81: Values of the read variables

At the function call all global variables are read out from the device and shown with their current value.

### 4.5.8 System variables of the signal processing

You reach this dialogue via < *Kommunikation* => *Systemvariablen der Signalverarbeitung* >.



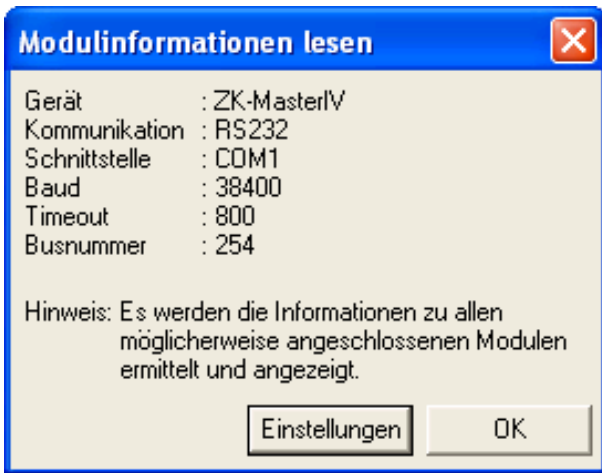
By clicking on "Read" you can read out the counter divisor, timeouts and cycles of the digital inputs.

Then, you can change the information by ticking it and apply it to the device firmware by clicking on "Write".

You should note that, if the value of a system variable is set on "0", the settings from the setup of the ZK-MasterIV are used. Otherwise, the entered value.

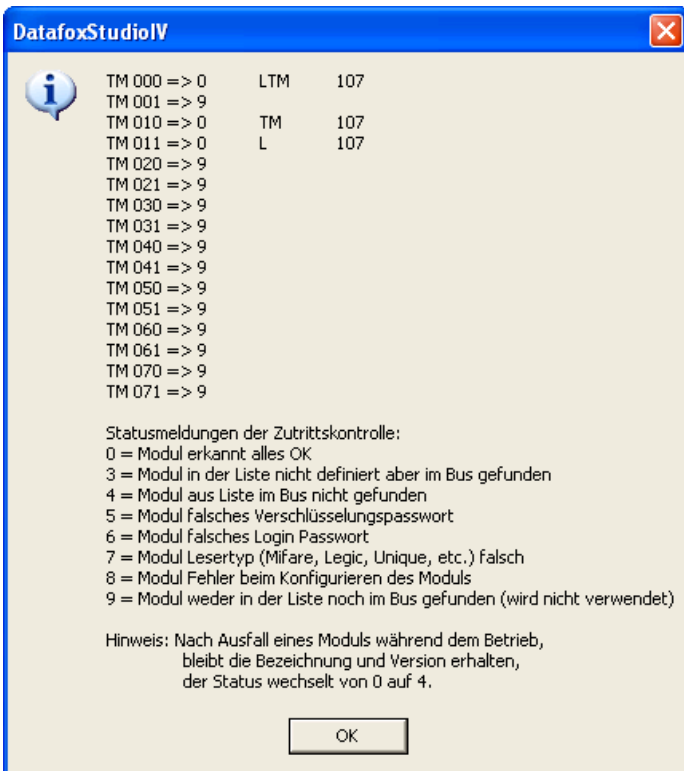
Figure 82: Dialogue system variables of the signal processing

4.5.9 Display state of the ZK-modules



Via this function it is possible to receive detailed information about the state of the access control modules. You can check, which modules of the access control have been recognized by the terminal and which state they have.

Figure 83: Read state of the ZK-modules



TM stands for Türmodul (door module), followed by the three-figure bus number. In the list the maximum number of modules that can be connected to the ZK-MasterIV is shown. The next number indicates the state of the module. In the next column the type of the module is shown, L stands for Leser (reader), TM for Türmodul (door module) and LTM for Leser mit Türmodulfunktion (reader with door module function). The lower field contains a small legend of the status messages.

Figure 84: State of ZK-module

#### 4.5.10 Work through batches

Via the function < *Kommunikation* => *Stapel abarbeiten* > the functions read data, delete data, set time, load setup, load lists and load access lists can be worked through chronologically. Further functions proceed automatically.

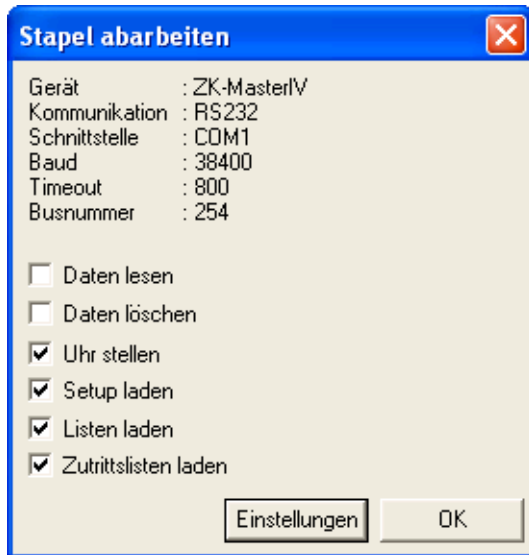


Figure 85: Work through batches

Depending on the activation/deactivation the respective functions are worked through.

After working through a reply for each activated function occurs.

Pay attention to the selection of the related setup if you have activated the option "Listen laden" (load lists). If you have not opened the right setup an error in the list processing occurs. All other options are executed faultless.

#### 4.5.11 GPRS configuration

Corresponding to the data of your provider you can create a \*.ini file for the GPRS configuration. The parameters that are necessary for the configuration of a GPRS/GSM connection are provided in the Ini-file. The Ini-file has the following structure:

```
; Standard values for GPRS modem (MC35i)
[MODEM_MC35i]

; Phone no. for dial-in
; _____
; T-Mobile, Vodafone, O2, E-Plus
PHONE = ""*99***1#"

; Access Point Name
; _____
; t-mobile GRPS = "internet.internet.t-mobile.de"
; vodafone GRPS = "web.vodafone.de"
; O2 GRPS = "internet"
; Contract customer
; E-Plus GRPS = "internet.eplus.de"
GRPS = "internet.internet.t-mobile.de"

; User name for internet dial-in
; _____
; t-mobile USER = "td1"
; vodafone USER = ""
; O2 USER = ""
; E-Plus USER = "eplus"
USER = "td1"

; Password for internet dial-in
; _____
; t-mobile PASSWORD = ""
; vodafone PASSWORD = ""
; O2 PASSWORD = ""
; E-Plus PASSWORD = "gprs"
PASSWORD = "gprs"

; Target configuration (port)
; _____
PORT = 80

; Target configuration (path)
; _____
HTTPSEND = "GET /oem/gprs/getdata.php?"

; Period of time between 2 alive-data records ALIVE = 300

; Period of time till the response of the server, otherwise disconnection
HTTPTIMEOUT = 15000

; Protokoll-Typ
HTTPTYPE = 1.1

; Target configuration (server)
; _____
; Target-IP or host name
; HOST = "192.168.0.1"
HOST = "www.datafox.de"
```



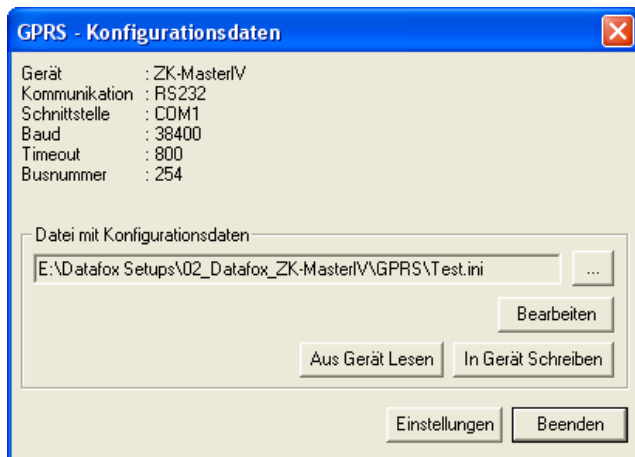


Figure 86: GPRS configuration

Via the GPRS configuration in the menu "Communication" you can read out the GPRS configuration data from a device, edit them and write them to a device or you can open an INI-file from your PC and edit it.

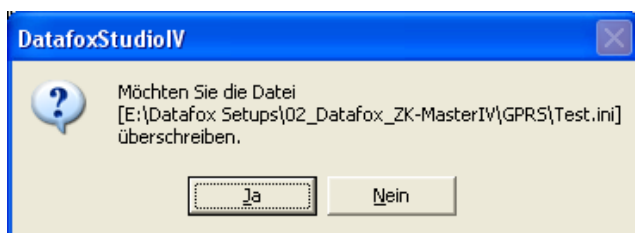


Figure 87: Overwrite configuration data

When you read out the data from a device, you have to set whether you want to overwrite the current file or write them to a now or another file.

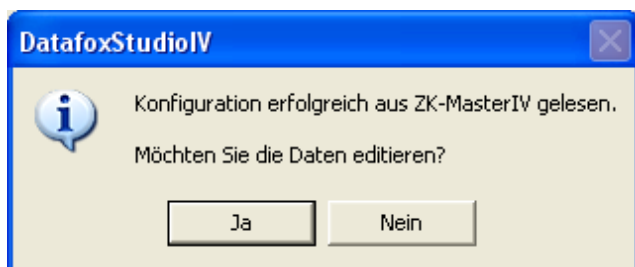


Figure 88: Reading of the GPRS configuration data

When the GPRS configuration was successfully read out from the device, you can select whether the data should be edited or be saved in the set INI-file.

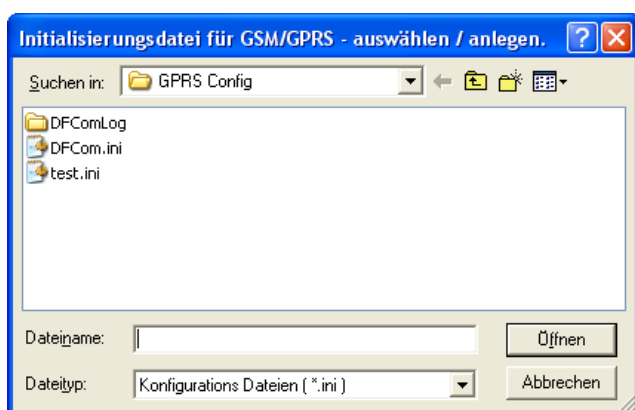


Figure 89: GPRS initialization file

If you have confirmed the dialogue in figure 87 with No, you have to select another file or enter a name if a new file shall be created.

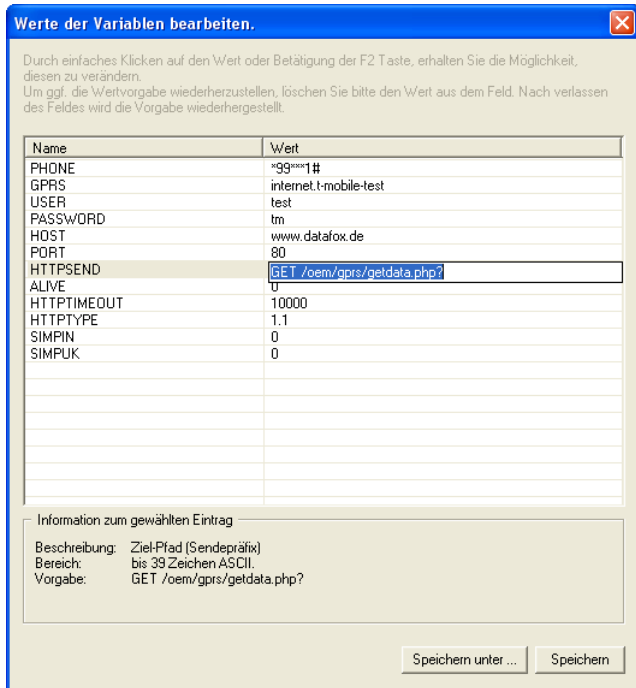


Figure 90: GPRS initialization parameter

In this dialogue you can edit the initialization parameter. Mark the line you want to edit by clicking on it. When the line is highlighted in blue, you can click on the selected parameter in the right column. An edit field opens where you can enter a new value. Additionally you receive information about the parameter. When all settings have been checked, the changes can be saved in the INI-file. Via the button *Speichern unter...* you can create a new initialization file.

When you have saved the data you can transmit them to the device via the dialogue in figure 86 with the button "Write in device". After the transmission you receive a status message.

#### 4.5.12 Device configuration BIOS

Because the ZK-MasterIV has no keyboard and display, it is necessary to make all configurations concerning the device bios via a PC. For this purpose, connect the device to the PC via the RS232 interface. TCP/IP is possible as well.

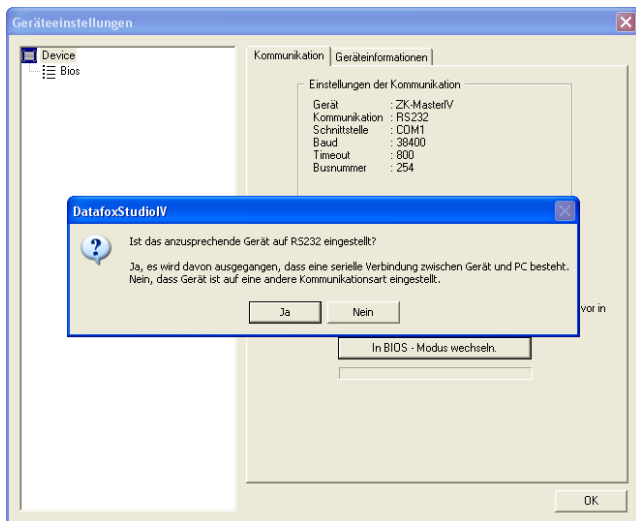


Figure 91: Device configuration (bios)

Check the settings of the communication parameter, type of device and communication. Open the dialogue for the device configuration (bios) via the DatafoxStudioIV menu *Kommunikation*. Click on the button "Switch to bios mode". When the device is already set on RS232, confirm the query with "Yes". Now, the bios mode is activated on the device. When another communication is set or the setting is unknown, confirm the query with "No". In this case, remove the device from the power supply.

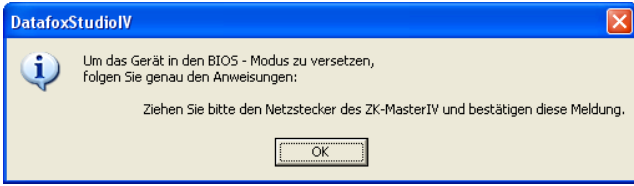


Figure 92: Activation of the bios mode

After having confirmed this message, you can re-establish the power supply for the device.

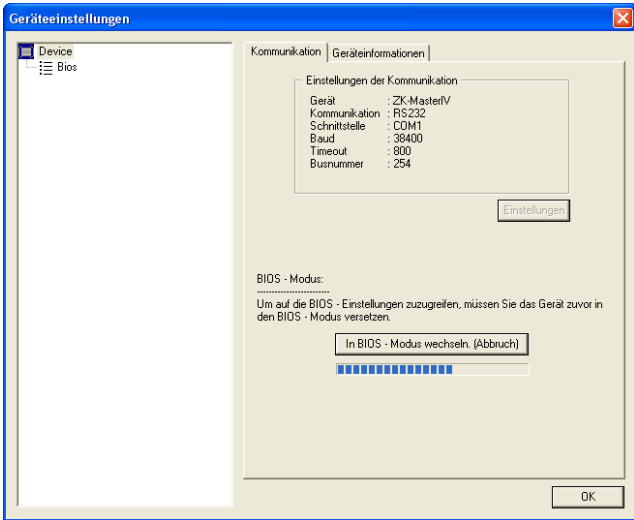


Figure 93: Activate bios mode at the ZK-MasterIV

The blue progress bar displays the activation process. After the execution you receive a status message.

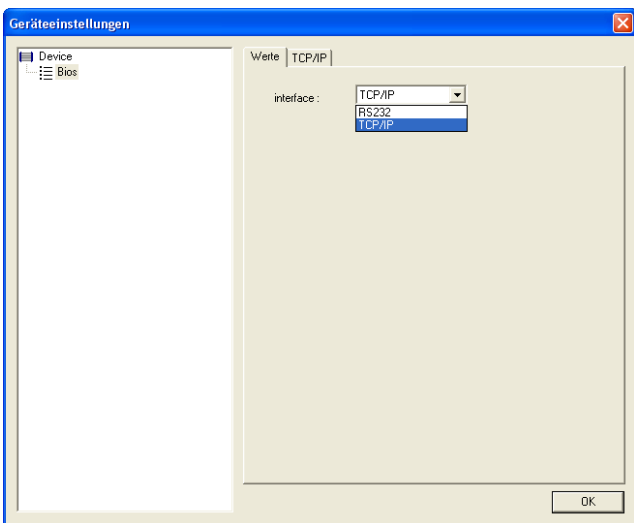


Figure 94: Device configuration (bios) - Interface

After a successful activation of the bios mode, all available interfaces for the main communication are displayed.

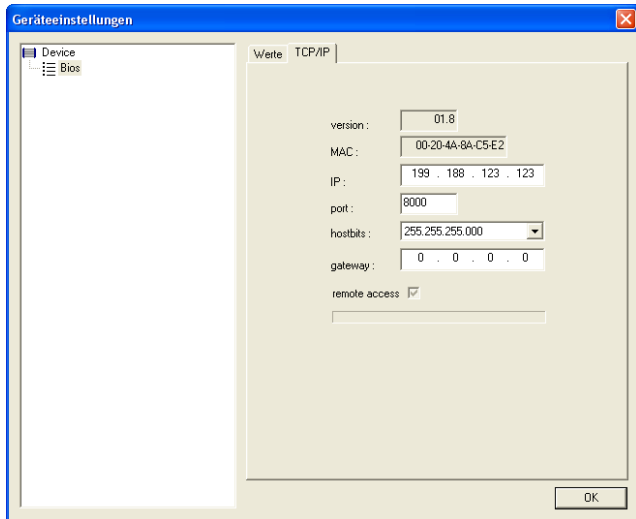


Figure 95: TCP/IP configuration

On the tab TCP/IP you can parameterize the IP address, network mask (hostbits), standard gateway and the option "remote access". If a DHCP is in the network, the IP address has to be set on "000.000.000.000". In this case the device obtains a dynamic IP address from the DHCP server.

Note for the option "remote access" that this parameter cannot be read out from the device. For this reason there are three states for the configuration. If it is ticked and active, the parameter is written in the device and "remote access" is activated. If it is not ticked the parameter is written in the device and "remote access" is deactivated. If it is ticked and deactivated (highlighted in grey), as shown in figure 95, the parameter is ignored and not written in the device.

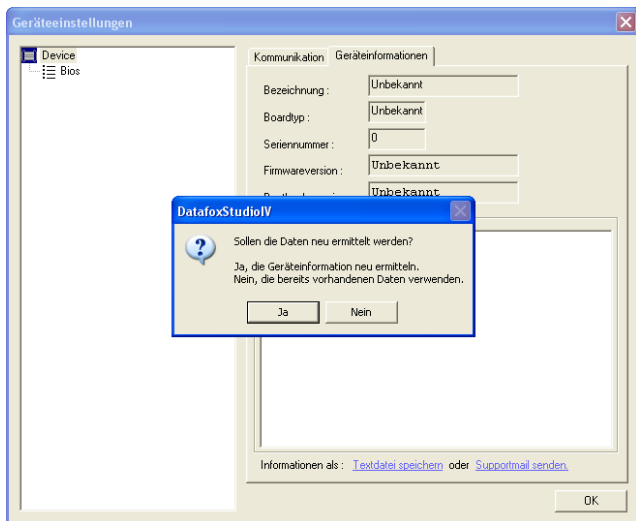


Figure 96: Device information

You also can receive information about the current hardware configuration via this dialogue. For this purpose, click on top on the right on device information.

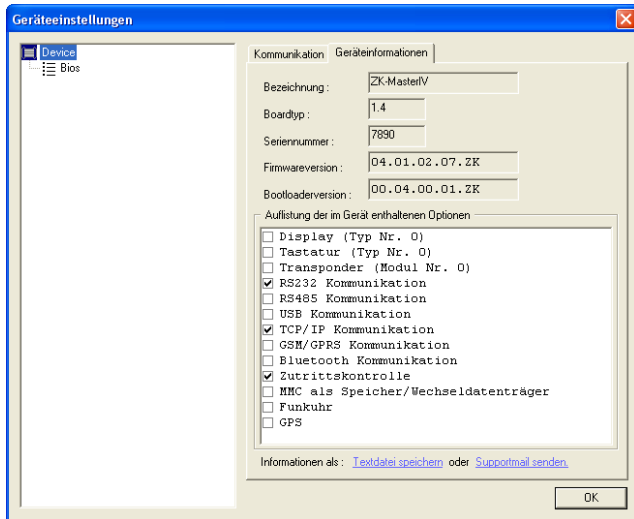


Figure 97: Show device information

If you have confirmed the query in figure 96 with "Yes", the hardware information of the device will be read and displayed in the list. All available hardware options will be displayed there. The set options are ticked.

### 4.5.13 Settings

Via the function  $\langle \text{Kommunikation} \Rightarrow \text{Einstellungen} \rangle$  you can select the parameter for a communication between a PC and the ZK-MasterIV. For all communications applies: at first select the device type. It can be set optionally whether only error messages should be output or whether the accessibility, should be checked via Ping before establishing a connection.

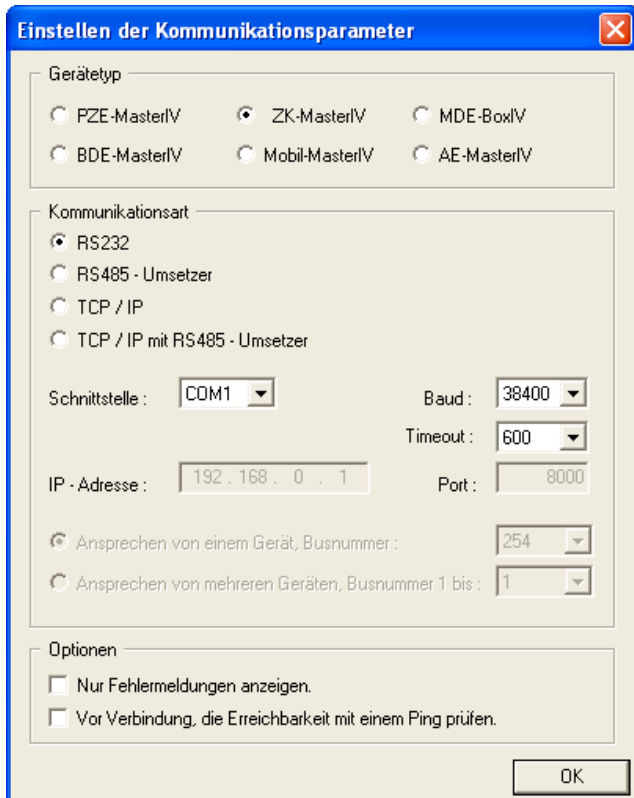
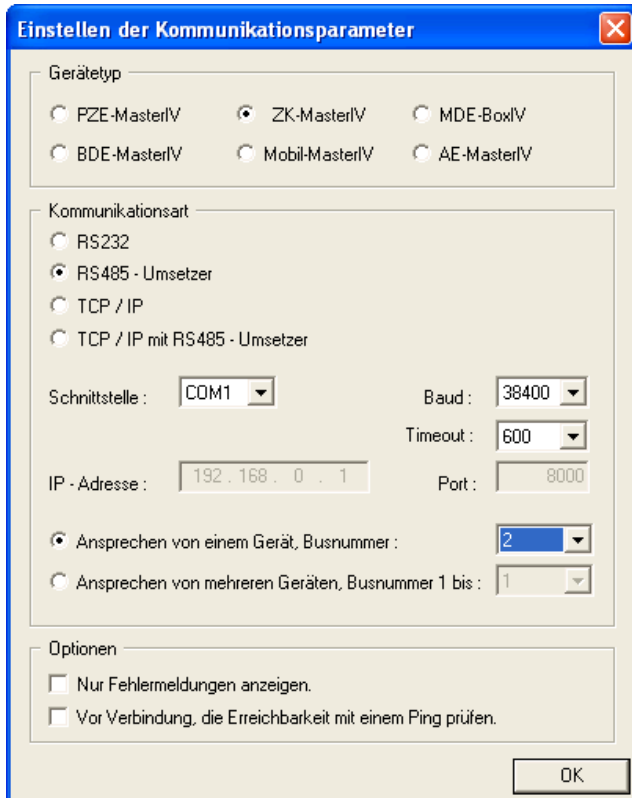


Figure 98: Setting of the RS232 communication

With the type of communication you set via which channel (transmitting medium) the communication should take place.

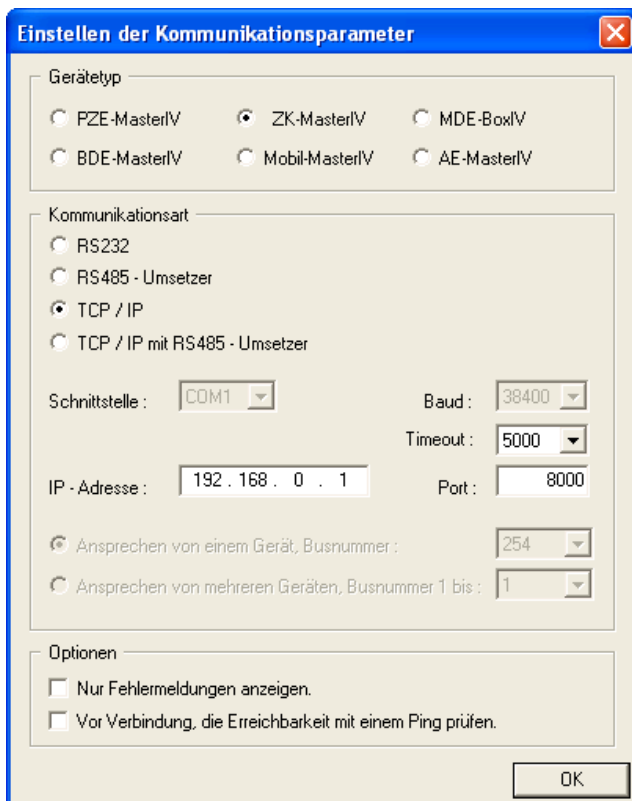
Dependent on the selected communication, the active parameter have to be set.

In case of RS232 the serial port (COM-Port), the baud rate (how many bits are transmitted within a second) and the timeout (time till the connection termination if no data arrive) have to be set.



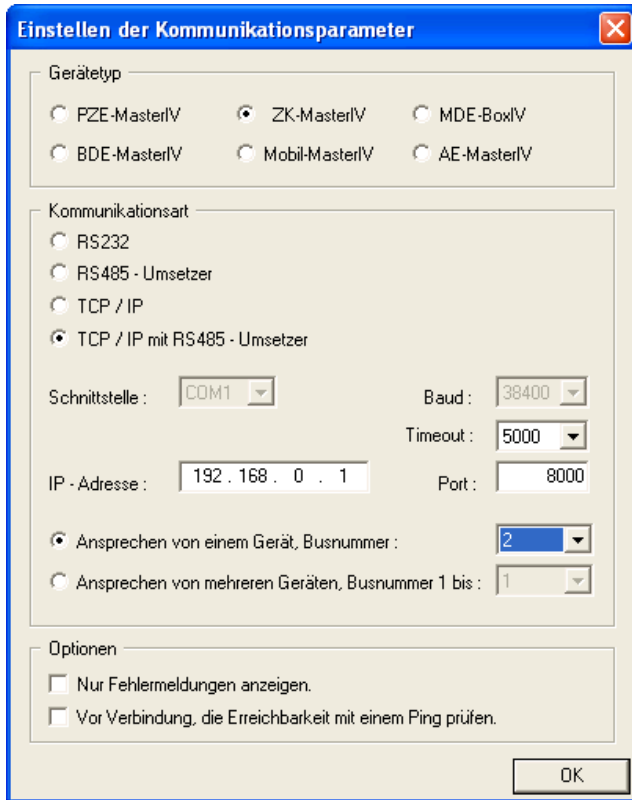
For a communication via a RS485 converter, in addition to the information of the RS232 communication you have to set if one or several devices should be activated. For a communication with only one device the bus number of the device is set (see system menu bios in chapter 4.5.12). Several devices can only be activated in a consecutive order of bus numbers, starting with bus number 1, and by giving the bus number of the last device.

Figure 99: Settings of the RS485 communication via converter



At a communication via TCO/IO the IP address of the ZK-MasterIV, the communication port and the timeout (in msec) have to be set.

Figure 100: Settings of the TCP/IP communication



In this case, analogous to a communication via TCP/IP the parameter have to be set and additionally it has to be set if one or several devices should be activated. For a communication with only one device the bus number of the device is selected. Several devices can only be activated in a consecutive order of bus numbers, starting with bus number 1, and by giving the bus number of the last device.

Figure 101: Settings of the TCP/IP communication via RS485 converter

#### 4.6 Menu Extra



**Note:**

You can and should check all displayed communication parameters at each dialogue that opens with one of the following function calls, and adjust them via the button Settings if necessary.

## 5 DatafoxStudiIV - Setup

### 5.1 Basics

#### 5.1.1 Planning

Before switching on the computer and creating the setup, the process of data collection and the setup structure should be planned. Only a few steps are necessary to do that. If you do the preparations carefully you can create the setup very fast.

On the graphic you can see the connections between parameterisation and result data. You may find secondary project support in the form of models on the Datafox CD.

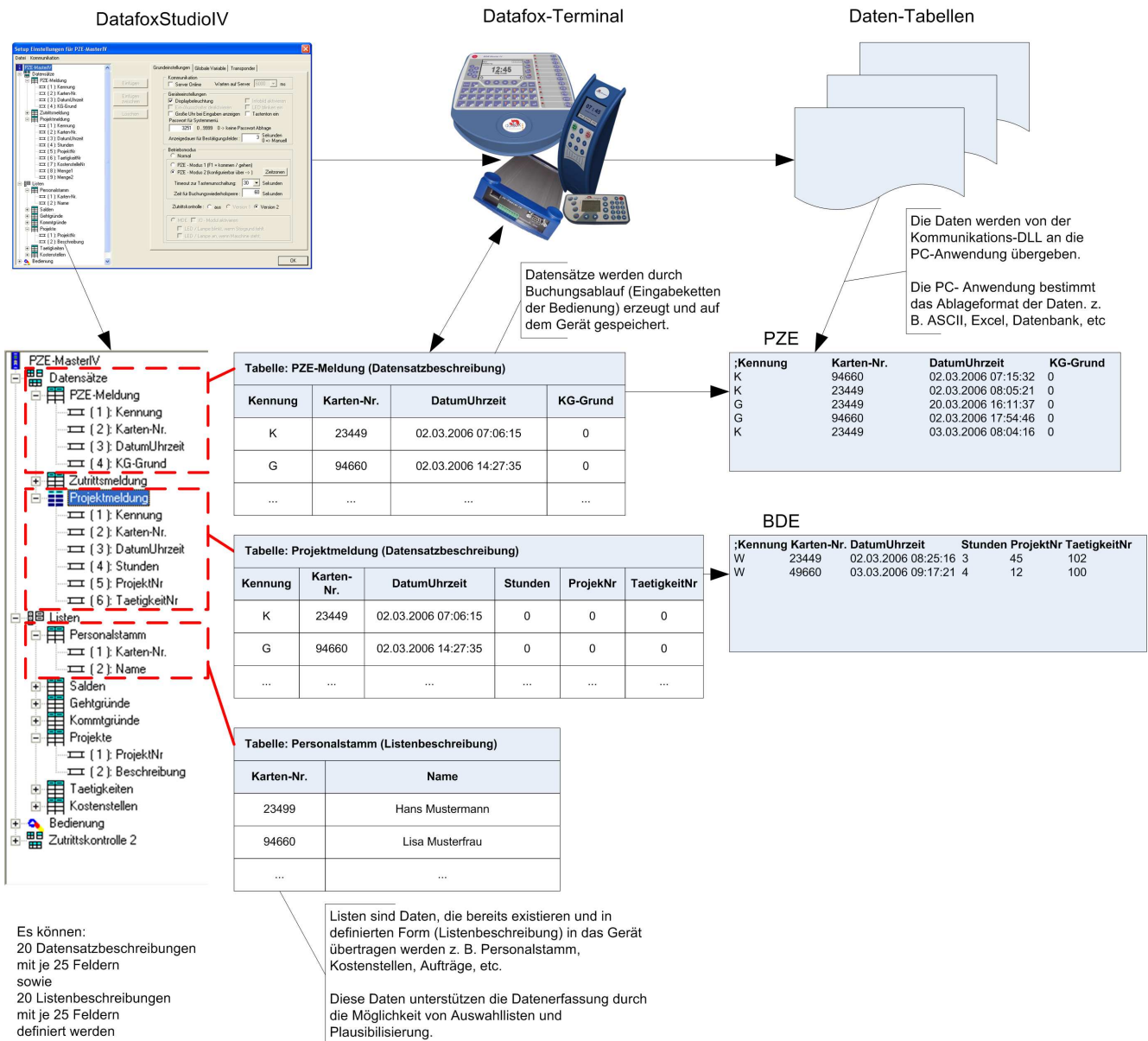


Figure 102: System relations



**Planning steps**

- ▶ Define all the tables for the data records that should be collected:  
field order, field name, field format
- ▶ Set the method of data collection for each field of a data record. In order to do this please use the operation (input chain fields):  
bar code, transponder, list, entering via keys, constants, global variables, etc. Combinations are possible
- ▶ In order to use lists you have to define this lists analogous to the data record descriptions:  
field order, field name, field format
- ▶ The most important step is the planning of the booking processes (input chains of the operation). To this step belong questions like this:
  - What is the best order to enter the fields?
  - Are loops or jumps labels necessary?
  - Are global variables necessary?
  - Are depending lists necessary? E.g. projects with specific occupations; if the project is selected, only the appropriate occupations can be chosen
  - Should the device switch off automatically after entering a data record?
  - ...



**Note:**

If the tree structure is very large, it might be arduous to open all the structures by clicking on it with the mouse. By using the following key combinations the tree structure also can be operated.

Shortcut	Funcion
* (on the keypad)	display all secondary files under the current selection
+ (on the keypad)	display the secondary files under the current selection
- (on the keypad)	fade out the secondary files of the current selection
↓	move down one position in the opened tree
↑	move up one position in the opened tree
→	open the following application level in a branch
←	close the complete branch

## 5.2 Functions of a setup

### 5.2.1 Basic settings



**Note:**

With the DatafoxStudioIV more than one device type can be configured. The functionality of the devices differs. Therefore it is important to select the device type at first. Only then it can be guaranteed that all functions are available while configuring and that they are not deactivated.

Depending on the chosen communication type some further settings have to be carried out. Please note, that all changes have to go well with the settings of the device (see chapter 4.5.13).

Für den ZK-MasterIV gibt es keine weiteren Grundeinstellungen.

From version 04.01.06. x can be put how much of the device memory should be used for records and how much for lists.

### 5.2.2 Global variables

Global variables are used as buffers within the device and do not depend on a data type. That way it is possible to transmit values, created within an input chain, to another input chain for reprocessing. At most 8 global variables can be defined in the ZK-MasterIV.

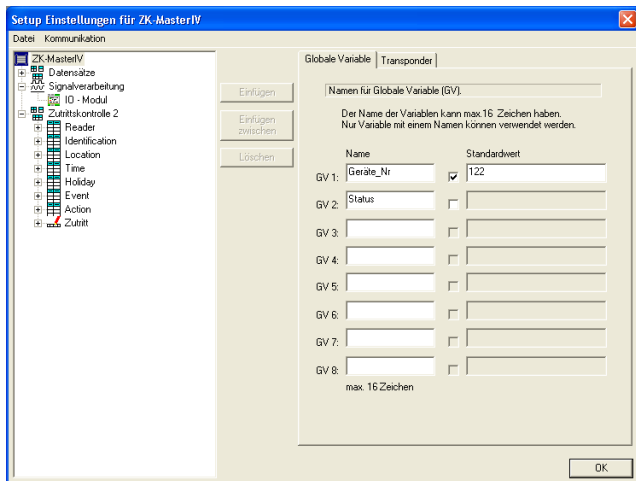


Figure 103: Setting of global variables

The use of global variables is explained in detail in chapter 5.3.


For testing purposes or also with the basic parameters (e.g. device-no.) it might be very useful, if the global variables are already preallocated in the setup.

Already while defining, the global variables can be preallocated with values (in the basic settings of the device via the register card Global variables, see figure 103). It is also possible to fill them with values via input chains within the term. If you access to the same GV repeated, writing, via input chains, the value of the GV is changed.

When a global variable is filled via an input chain you have to differ to cases: Either you fill the GV and create a data record concurrently, or you fill the GV without creating a data record. In the second case please note, that there should be no connection to any data record description.

When inputting GVs using the function Normal, you can carry out a format check via the register card Expanded. Such a test is not available for other input functions. That is not necessary, because there the data formats are set in advance.

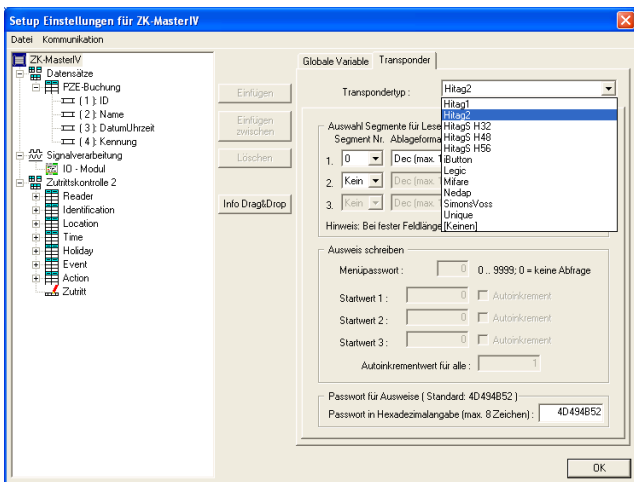
**Note:**



- When you transmit a new setup, it is possible to delete global variables and their values. In order to do this you have to activate the appropriate option.
- If you want to reset one or all GVs to a defined value (e.g. at clocking-off), you have to create an input chain with the appropriate fields. Use the function Constant. Via the configuration of the time zones you can set, when this input chain resets the GVs.

### 5.2.3 Transponder

Transponder readers are provided as external module, e.g. TS-TMR33. You can set the transponder reader via the settings in the setup (see figure 104).



When configuring the transponder please mind the provided information about the current transponder type.

The reading system is set via the transponder type.

Figure 104: Settings of the transponder

At the moment the following transponders are supported by the ZK-MasterIV Fields on the transponder				
Frequency	Type	Module	Fields on the transponder	Comment
125 KHz	Unique	TMR33,	Fixed 13-digit number	Only reading possible
125 KHz	Hitag1	ProxLine MCR, PHG-Voxio oder -Relino	64 segments each 4 byte: 0 = Fixed number, only reading 1 to 31 = Passwords, 32 to 63 = available.	The available segments can be used e.g. to save a firm identification, a card number, an account for canteens etc. PHG supports at most 3 segments with Hitag1 and 2, with Titan only the serial number.
125 KHz	Hitag2	(Switch over in DatafoxStudioIV)	8 segments each 4 byte: 0 = Fixed number, only reading 1 to 3 = Passwords, 4 to 8 available.	
125 KHz	HitagS		1 - 63 available	
125 KHz	Titan EM4450		34 segmentes: 0 to 2 = Password 3 to 31 = available 32 to 33 Serial/Device ID	
13,56 MHz	Mifare	Mifare, PHG-Voxio oder -Relino	16 segments available	The high speed and the large memory capacity are also favourable. So this transponders are very suitable for biometry.
13,56 MHz	Legic	Primo, PHG-Voxio oder -Relino		
—	iButton	iButton	Fixed 15-digit Number	

Table 21: Overview over supported transponders

Various possibilities of configuration are available for the DatafoxStudioIV, depending on the chosen transponder type.

## 5.2.3.1 Transponder reading systems

Read		
Type	Frequency	Module
Unique	125 kHz	TSR20, TSR21, TSR30, TSR32, TSR33
Hitag1	125 kHz	TSR21, TSR32, TSR33
Hitag2	125 kHz	TSR20, TSR21, TSR30, TSR32, TSR33
HitagS H32	125 kHz	TSR21, TSR32, TSR33
HitagS H48	125 kHz	TSR21, TSR32, TSR33
HitagS H56	125 kHz	TSR21, TSR32, TSR33
Titan EM4450	125 kHz	TSR20, TSR21, TSR30, TSR32, TSR33
Mifare	13,56 MHz	Mifare
Legic	13,56 MHz	Primo
iButton	—	Dallas Semiconductor DS9092
PHG	125 kHz sowie 13,56 MHz	Aperio, Relino

Table 22: Transponder read

**TMR33 supported by GIS:**

Unique (Serial number)

Hitag1 (max. 3 segments)

Hitag S H32 (max. 1 segments)

Hitag S H48 (max. 3 segments)

Hitag S H56 (max. 3 segments)

Hitag2 (max. 3 segments)

EM4450 (max. 3 segments)

**Please note the following when using Mifare:**

The value-format is not supported.

You can only read the data-format with the key-A.

You can read and write the default-format with key-A.

## Unique

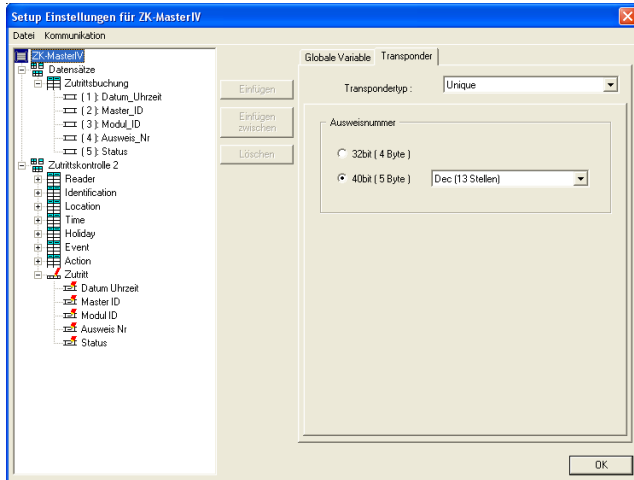


Figure 105: Unique transponder

Unique is a pure reading system. The card number is a worldwide well-defined ID and is used in all conceivable fields. A 64bit information is saved on the card. For the well-defined ID only 40bits are used. The remaining bits are amongst other things used for a checksum. When using Unique in DatafoxStudioIV the value of the card number (ID) (as 40 or 32bit-value) can be used for further processing.

## Hitag1

Hitag1 is organized in 16 blocks at 4 segments each. Each segment has a length of 32 bits. The block numbers 4 to 7 can be saved with a password (secret) or used without one (public) optionally.

!

**Caution:**  
DatafoxStudioIV supports only the segments 0 and 8..63. The segments of 32..63 can be read and written always, the segment 0 can be read always. Depending on the content of the segments 1..7 it might be possible, that the segments 8..31 cannot be read or written.

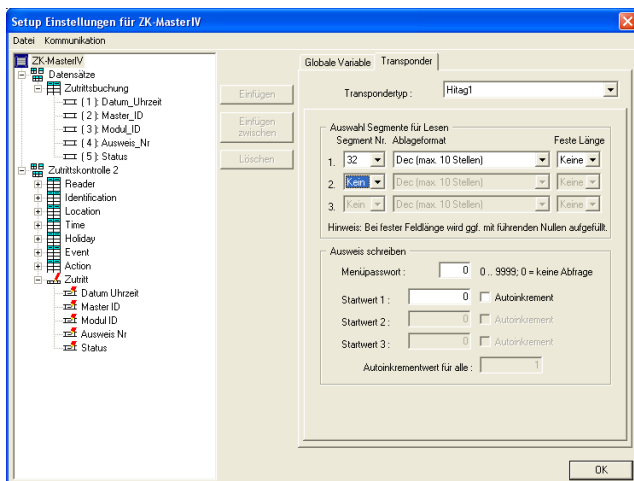


Figure 106: Hitag1 transponder

At most 3 segments are available for concurrent processing. You can select them in the DatafoxStudioIV under Transponder via the segment number.

Via the filing format you set how the 32bit-value is used.

When you select Fixed length the read card value is cut to the set number of digits and is filled up with zeros (0) left-sided, if necessary.

For the writing of the cards an initial value per each segment can be set. You can activate the option Autoincrement value behind the current initial value. Then the current segment value is increased by the value indicated under Autoincrement value after every write operation. The initial values of the segments

can be edited in the device-BIOS. The set autoincrement value is only displayed in the device-BIOS and cannot be changed on the device itself. The writing of cards can be saved by a menu password.

## Hitag2

Hitag 2 is organized in 8 segments. Each segment is 32 bits long.

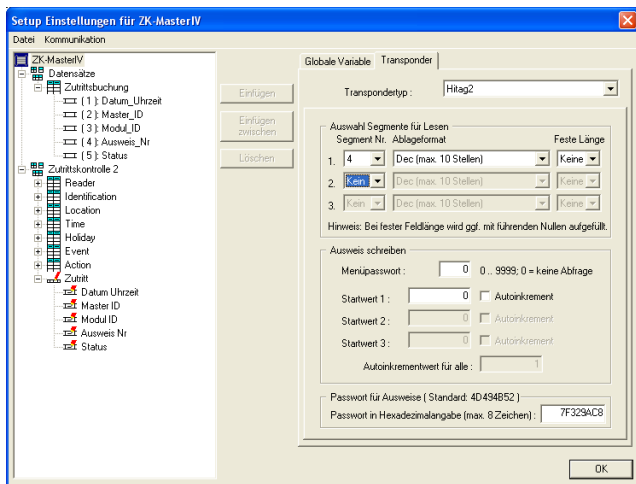


Figure 107: Hitag2 transponder

At most 3 segments are available for concurrent processing. You can select them in the DatafoxStudioIV under Transponder via the segment number.

Via the filing format you set how the 32bit-value is used.

When you select Fixed length the read card value is cut to the set number of digits and is filled up with zeros (0) left-sided, if necessary.

For the writing of the cards an initial value per each segment can be set. You can activate the option Autoincrement value behind the current initial value. Then the current segment value is increased by the value indicated under Autoincrement value after every write operation. The initial values of the segments can be edited in the device-BIOS. The set autoincrement value is only displayed in the device-BIOS and cannot be changed on the device itself. The writing of cards can be saved by a menu password.

## HitagS

When using this method you differ between "HitagS H32", "HitagS H56" and "HitagS H48".

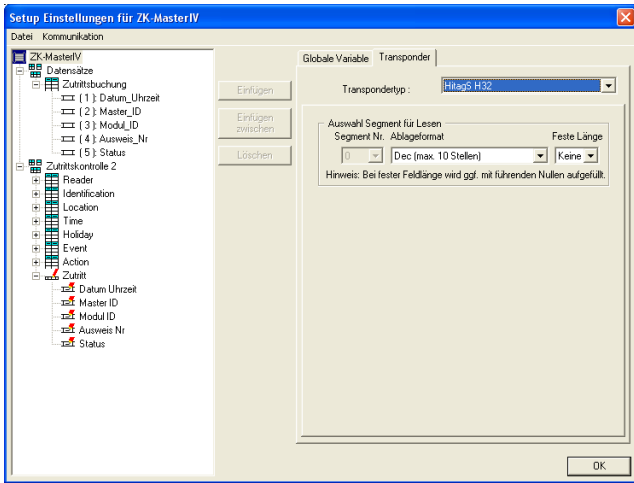


Figure 108: HitagS H32

HitagS H32 means, that this transponder has just a 32bit-value (= serial number of the card) (see Unique).

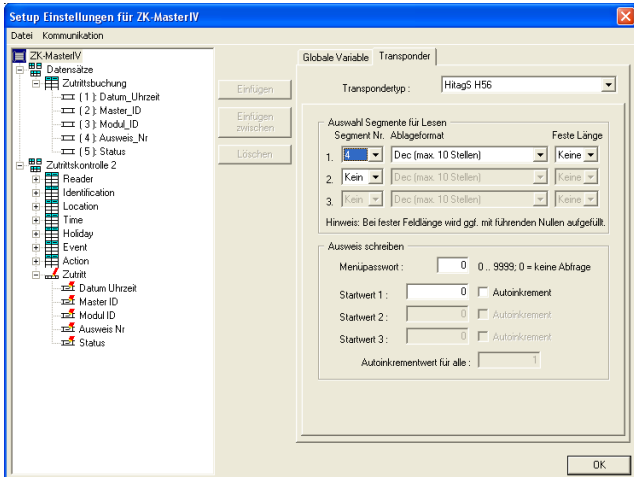


Figure 109: HitagS H56

The H56 means, that this transponder has 8 registers for a 32bit-value each, altogether 256 bit (see Hitag2).



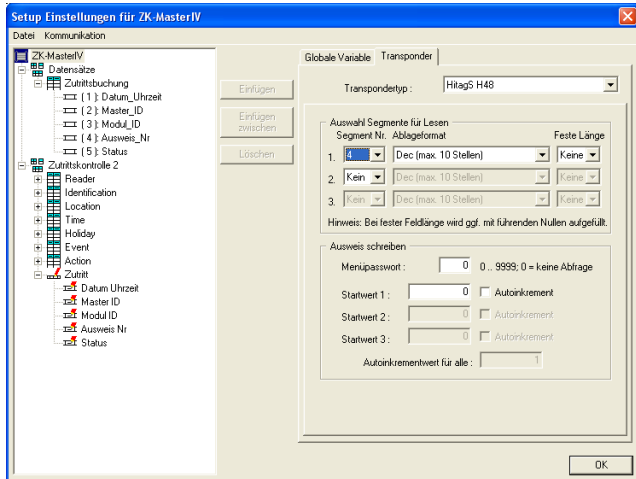


Figure 110: HitagS H48

The H48 means, that this transponder has 64 registers for a 32bit-value each, altogether 2048 bit (see Hitag1).

## Titan

Titan (EM4450) is organized in 34 segments. Each segment has a length of 64 bits. You can find the serial number in segment 32.

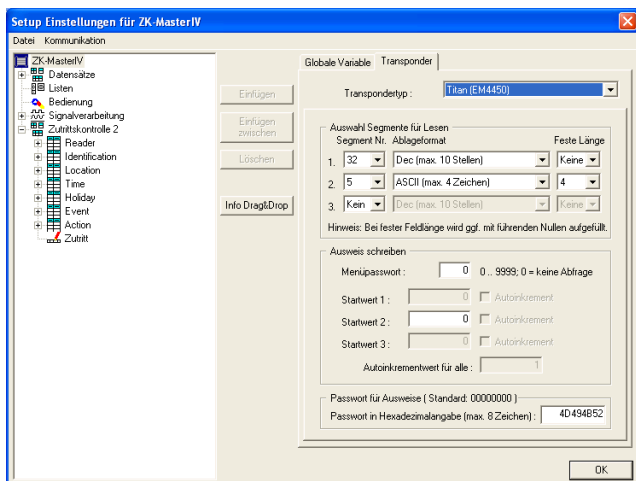


Figure 111: Titan EM4450 transponder

At most 3 segments are available for concurrent processing. You can select them in the DatafoxStudioIV under Transponder via the segment number.

With the filing format you set, how the 64bit-value is used.

When you select Fixed length, the read card value is cut to the set number of digits and is filled up with zeros (0) left-sided, if necessary.

For the writing of the cards an initial value per each segment can be set. You can activate the option Autoincrement value behind the current initial value. Then the current segment value is increased by the value indicated under Autoincrement value after every write operation. The initial values of the segments can be edited in the device-BIOS. The set autoincrement value is only displayed in the device-BIOS and cannot be changed on the device itself. The writing of cards can be saved by a menu password.

## **Mifare**

Mifare is organized in 16 sectors at 4 blocks each (each per 16 Byte). Each fourth block is used to encrypt the data on the transponder. It is partitioned into a key-A and a key-B and contains a password (each 6 byte long) for write- and read permission as well as the access condition, the media types are defined in. Depending on the application, all blocks of a sector can be available either in default-format (i.e. the key-A is the read- and write protection key) or in data- or rather value-format (i.e. the key-A is the reading password and the key-B is the master key for reading and writing). At the moment the Datafox devices (up to version 4.1.4.xx) support only the default-format.

## **Legic**

Legic is used only in the German speaking areas. Both spanned and unspanned memory cards are provided. On the unspanned memory card the data are read by means of position- and length indication. It is impossible to write on such memory cards.

On the spanned memory cards you have to set not only the length but also the segment, the data are read from.

## **iButton**

iButton is a contact reading system. The iButton has only a serial number, which is read, when a contact between iButton and transponder takes place.

### 5.2.3.2 Function upgrading for Mifare transponders

#### 5.2.3.2.1 General information

The function Autologin always works in this version. If no password is entered, the default password by Philips or Infineon is used. If a password is entered, at first a login as key A is carried out and if that fails, this password is used as key B. Autologin is active only for reading.

#### 5.2.3.2.2 Global settings

##### Mifare

Three password groups are provided. Password group 1 is used for the global settings. Range 2 is freely available, range 3 can be used with the restriction, that here the passwords of the old card (for rewriting the Access Conditions Bits of the sector trailer in the BIOS menu) are logged.

For the ASCII-format the value with the given length is written on the card, a zero-termination is not written on the card. If there are any zeros within the given length, they are written on the card.

For the ASCII-format the value with the given length is read from the card, a zero-termination is added after the given length. Thus, the maximum length, possible for the card, used completely.

All Mifare standard cards can be used. When using 1kByte cards all sectors can be used, when using 4kByte cards only the first 16 sectors (out of 40) can be used.

##### Autologin function

In the previous version 04.01.04.xx the Autologin was active non-stop; only a few users knew this and used it. In the version 04.01.05.19 (and higher) the Autologin works in a different way. At activation all 6 passwords, that are given, are used until a login was successful. This function allows only the reading of the card with various passwords; when writing on the card the password has to be correct. If Access is used, the Autologin function cannot be used, because the access reader permits only one reading password for security reasons.

##### Access Conditions Bits

The Access Conditions Bits are logged on the sector trailer, the fourth block of a sector. Each sector can have its own password key A and B, also the access rights can be set for each sector and even for each block. The sector Trailer is structured as follows:

The sector Trailer cannot be read out via the setup functions. Only the blocks 0 to 2 are accessible in order to read and write data. The Access Conditions indicate the block format and the access rights of the block of a sector. The Value format is not supported by the firmware, but this can be set optionally. You should pay special attention to the Access Condition (B3), because the settings of the sector Trailer cannot be changed afterwards, it is write-protected then. If you are not sure, you should use the default settings of the producer.



##### Caution:

The Access Conditions Bits do not change the settings of the password use in the groups 1, 2 or 3. Here you have to pay attention, so that the settings correspond to the ACB. A set write-protection of the sector Trailer cannot be cancelled.

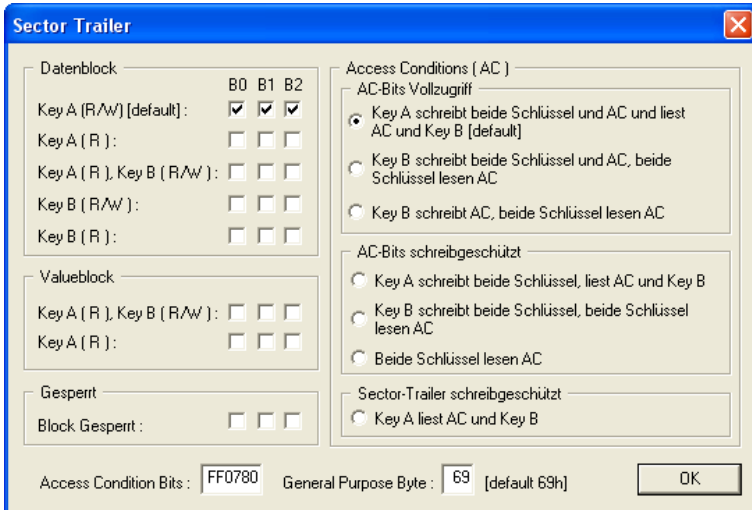


Figure 112: Sektor Trailer

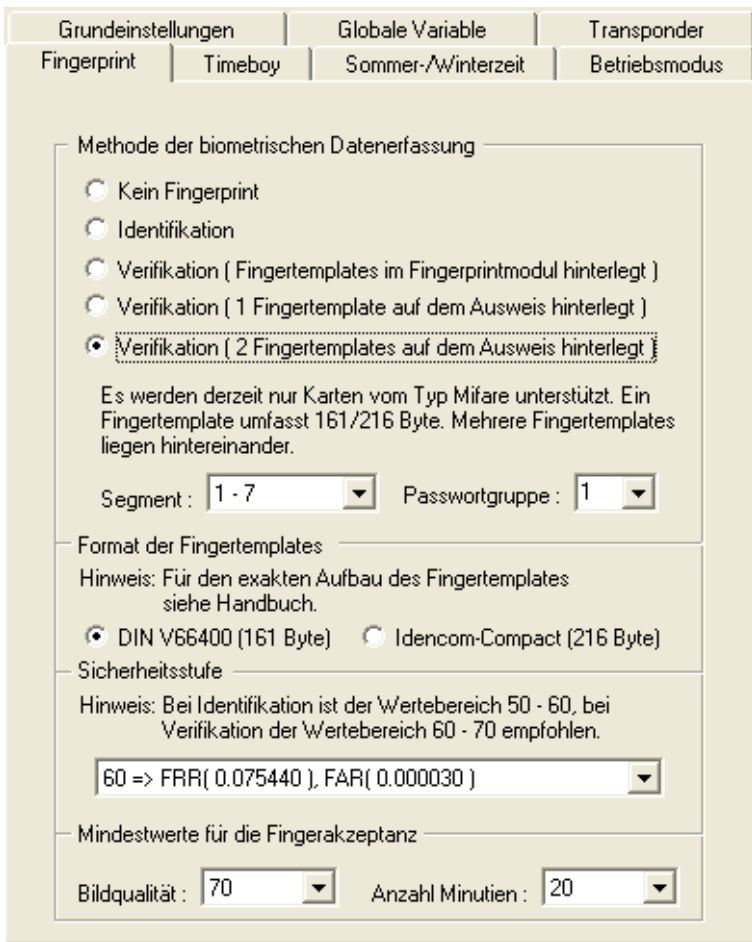
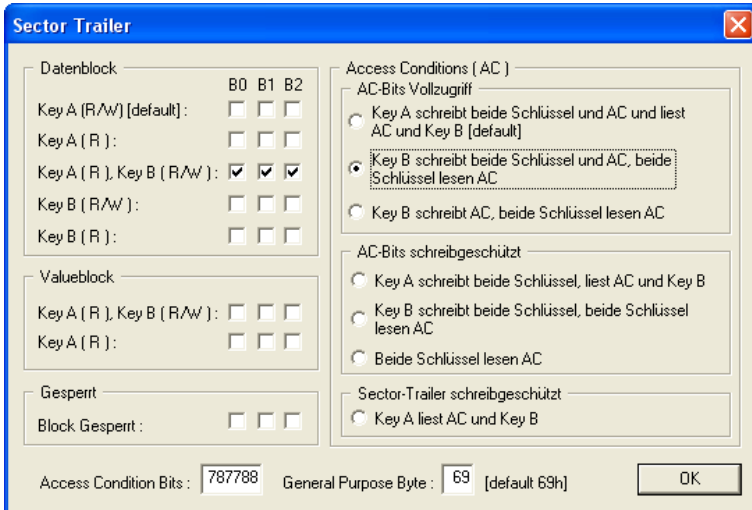


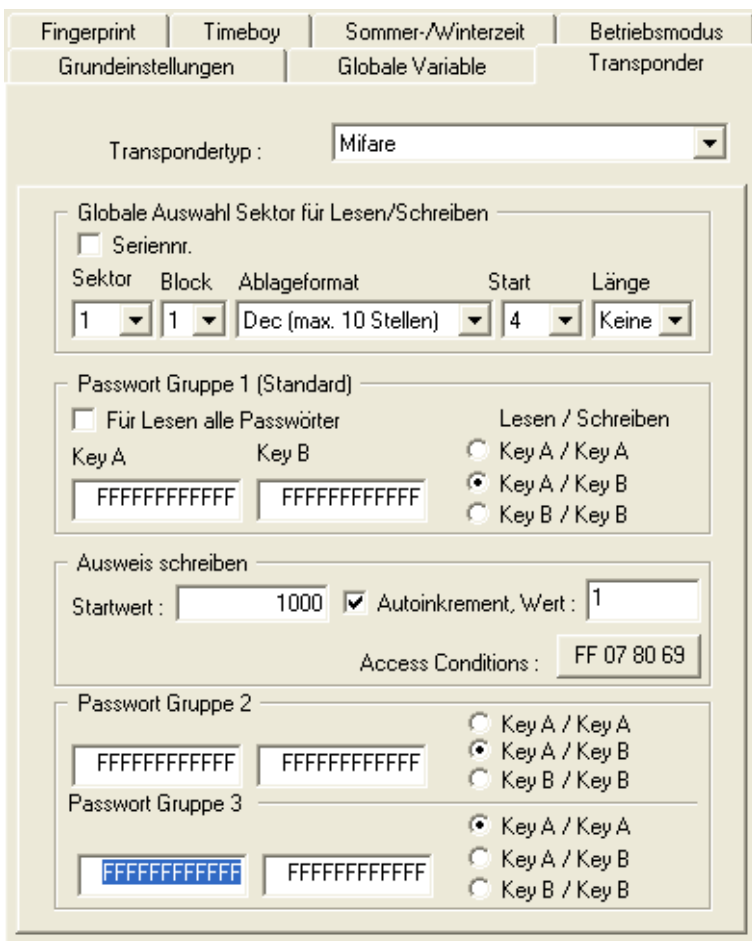
Figure 113: Example of a card

The card with the set default password key A FFFFFFFFFFFFFFFF for reading and writing with the ACBs FF078069 is new.. The card should have an ID number (32-bit as decimal value with leading zeroes, 10 digits) in the range sector 1 block 1, and a data range for fingerprint in the sectors 2 to 10. The range for the ID number uses the password group 1 with key A (reading key) and key B (writing key); the range for the fingerprint uses the password group 2, also with key A (reading key) and key B (writing key). In that case the ACBs have to be changed.



The ACBs (Access Condition Bits) should have a value of 78778869.

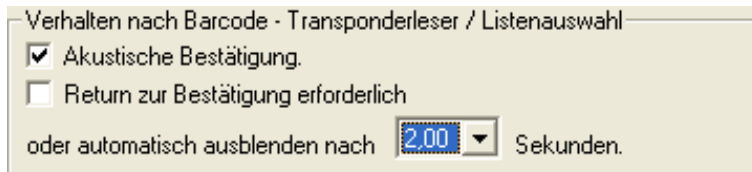
Figure 114: Sektor Trailer



In order to set the card on the values, intended for the use in the setup, the password group 3 has to contain the old passwords; in this example key A with FFFFFFFF as reading and writing key. Via the transponder menu the card can be set newly, but the formatting sector has to be activated. The ID can be set via Write data on card, the field Fingerprint via Fingerprint sector trailer. Now the card possesses different reading and writing passwords for fingerprint and ID, that are only known to you and the terminal.

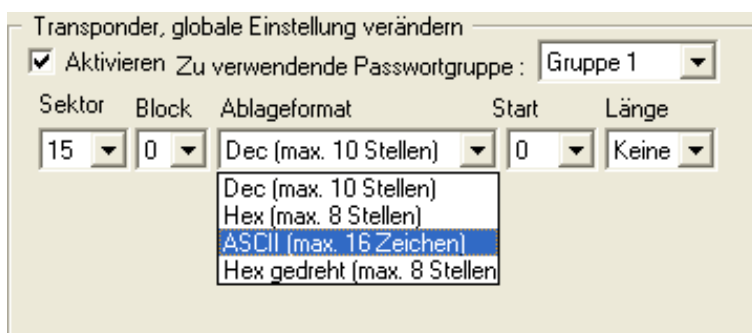
Figure 115: Password definition

### 5.2.3.2.3 Function normal



New for this field function is the switching-on and -off of the acoustic signalisation. The background is, that the last access to the transponder shall create a beep, in case of carrying out several reading and writing processes within one input chain.

Figure 116: Behaviour after Barcode - transponder reader



On the field Mifare some alterations were carried out, so that now not only an ASCII string can be read, but also binary values (as already possible at other transponder processes). It is important, that the password group is set correctly, so that the data can be read.

Figure 117: Behaviour after Barcode - transponder reader

### 5.2.3.2.4 Transponder value write, also for Hitag1, Hitag2 and Titan

Only values of global variables can be written.

Note for the user: With Hitag several segments can be used. If these segments use different formats, the number of digits has to be set under Decimal (except for the use of only one segment). Otherwise, the data might be written on an other range than desired.

The page Expanded has the same structure as the one for field function Normal.

### 5.2.3.2.5 Transponder menu

The transponder menu is different only on the register card Mifare. The function Formatting sector was added to the hitherto existing functions/ menu items. The activation of this new function causes, that a card with key Ax and key Bx and its current ACBs is overwritten with the values of key A and key B of field 1 and with the ACBs of block 4, set in the setup. In order to carry out a login with the correct passwords, key Ax and key Bx have to be set in the password group 3. All this is important, if you want to create a new password for a card, that is new/ unused or even already used.

Terminals with fingerprint If the terminal is equipped with fingerprint and Mifare, the menu item "Fingerprint field sector trailer" is displayed in the transponder menu. Here the sectors, with the settings of the password section, edited under Fingerprint, are set. If Formatting sector is active, the passwords and the ACBs are set; if this option is deactivated, only the passwords are set. For the logging-in password the field 3 is used. The number of sectors, that are not accessible, is displayed at the end of the formatting

process. The reason for this are the different Access Conditions of the single sectors. Here the terminal will not help you. Such error sources have to be eliminated before, or you have to make sure, that the cards were not used yet. In that case such an error does not occur.

Conclusion If Formatting sector is deactivated, only the value is written on the card under Write card, on the fingerprint field Sector trailer only the passwords for the memory range of the fingerprint templates are set. If Formatting sector is activated, both passwords under Write card and block 4 of the segment with Access Conditions on the fingerprint field Sector Trailer are written newly. If the fields to be written are write-protected, an error message is displayed.

You may find further information about Mifare under <http://www.mifare.net/> or [www.nxp.com](http://www.nxp.com) Products => Identification => MIFARE => MIFARE Classic.

### 5.2.3.3 Application possibilities for Hitag-transponder

All Hitag-transponders have got a fixed serial number in segment 0 and further available segments. You may find information about number, size and function in table 21. There is the possibility to use different segments. So you have several possibilities to use them with PZE and ZK. In the following you may find 2 examples for the possible use of PZE and ZK as well as the advantages and disadvantages.



#### Note:

You recommend the safer method with lists in the terminal. When using ZK lists they are necessary anyway.

#### Example 1.

ZK-MasterIV setup for Hitag2 with firm code in segment 4 and personnel number in segment 5.

#### Operation:

The firm code is filed in segment 4. When reading the card a format check is carried out, e.g. 010101\* for the customer ID 10101. The first 0 is created, because the fixed field length is 6. That means, even if the customer ID becomes a 6-digit number, the process still works.

The personnel number is filed in segment 5 (card number = personnel number).

Security is created by the firm code exclusively. Of course a further list could be loaded. But this would not be an improvement, because the clearness of the card number cannot be guaranteed.

The cards can be programmed via the terminal or the desktop reader TS-WR34\_USB article-no. 222001

#### Advantages:

No permanent staff lists have to be transmitted to the terminal.

#### Disadvantages:

Overlappings might be possible, if the firm code is not well-defined. That can happen, if you forget to set the setup for the project or if another producer uses the same method. Different accounting programs use different formats for the customer ID. The setup has to be set customer-specific.

- ▶ Under Transponder the project number/customer ID has to be input.
- ▶ The format check has to be set in each input chain.

Each card has to be programmed.

**Example 2.**

ZK-MasterIV setup for Hitag 2 with card number in segment 0 and check on lists.



**Operation:**

Only the well-defined serial number (already programmed by the producer) in segment 0 is used.

Security is created by a check of the permanent staff lists (as standard with Unique).

**Advantages:**

The process is absolute safe because the well-defined serial number is used.

The setup does not need to be adjusted to each costumer, i.e. the same setup can be used for various projects/costumers.

The cards do not need to be programmed.

All free fields are available for other uses (canteen, drinks dispenser, firm equipment etc.).

While bookings are carried out, the name of the person can be displayed.

**Disadvantages:**

You have to load the lists, that should be controlled on the device compulsorily. (Alternative: This can also be done via an online check with the server application.)



**Note:**

Datafox offers a desktop reader with USB-connection to read the serial numbers into the PZE-software. By the keyboard emulation software the reader reacts like a keyboard. The cursor is put to the field Card number and the transponder is read. The number in the set segment is read and written to the position of the cursor.

**5.2.4 Creating data record descriptions**



**Caution:**

When creating data record descriptions please note the following restrictions:

- At most 25 data fields are admissible per each data record description.
- The field length of date and time is set in advance by the format fix.
- Numeric character fields and ASCII-fields with a firmware release smaller than 04.01.03 are limited to 20 characters, the following firmware versions can save up to 40 characters in the fields.
- The total length of a data record is limited to 230 byte.
- At most 20 data record descriptions can be created.

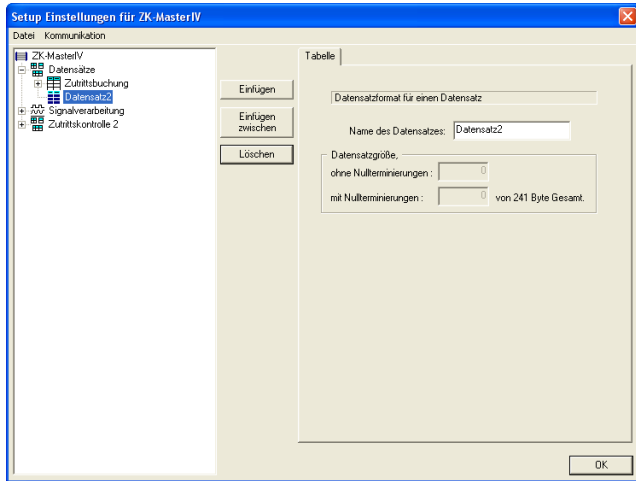



Figure 118: Creating a data record description

When creating new data record descriptions under the element Data records please proceed as follows. Select the element Data records in the tree structure (it is highlighted in blue then). Via the button Paste a new data record description is created; the tree structure is expanded to a new entry. If several data records exist you can set the position of the new data record via the button Paste between.

In order to name the new data record, click on it in the tree structure. On the right side the details about this data record are displayed. There you can enter the new name.



**Note:**

All entries are applied automatically and do not need to be saved explicitly. Via the button OK you leave the edit dialogue and return to the setup dialogue.

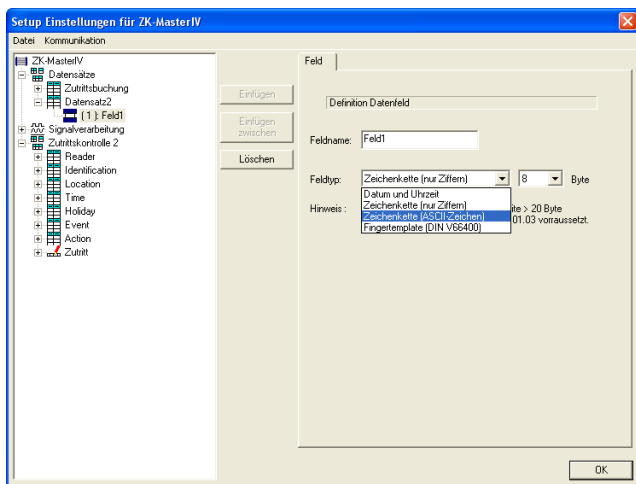


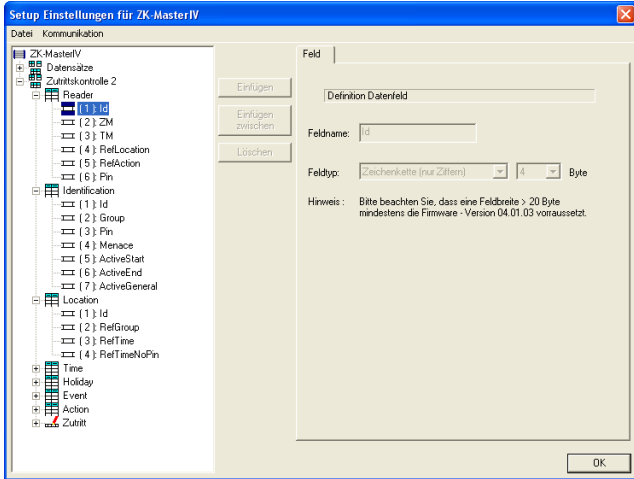
Figure 119: Creating data fields

For each data record appropriate data fields can be created and the field characteristics can be defined. This procedure is the same as when creating new data records.

The data type Date\_Time is defined with a fixed length. When using strings you have to give an indication of length additionally.

### 5.2.5 Creating list descriptions

Lists provide a defined data base. You can compare them with the combo-box of a PC application.



The list descriptions for the access control are provided by the system. Via the DatafoxStudioIV you can review the structure of the lists (configuration, field names, data type, size).

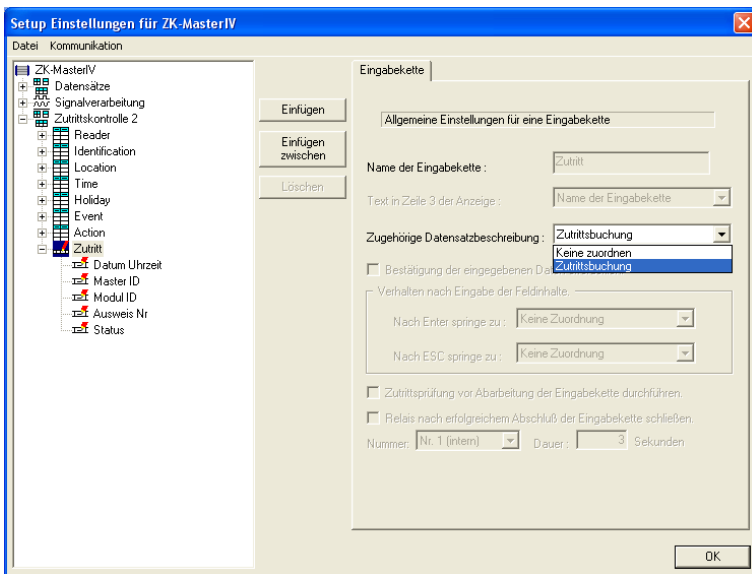
Figure 120: List description of the access control lists

### 5.2.6 Creating a user guidance

As explained in chapter 3.4 operating the terminal via keyboard is impossible. Therefore the ZK-MasterIV does not possess a actual main menu. Nevertheless you need an input chain (with the appropriate logic) to carry out access controls.

#### 5.2.6.1 Defining input chains

An input chain defines a series of data fields that are entered on the device or filled automatically via collection- or control routines. Via this input chains the data records are filled by the device (see chapter 5.2.4). If several input chains are created under one menu item, they are worked through one after another.



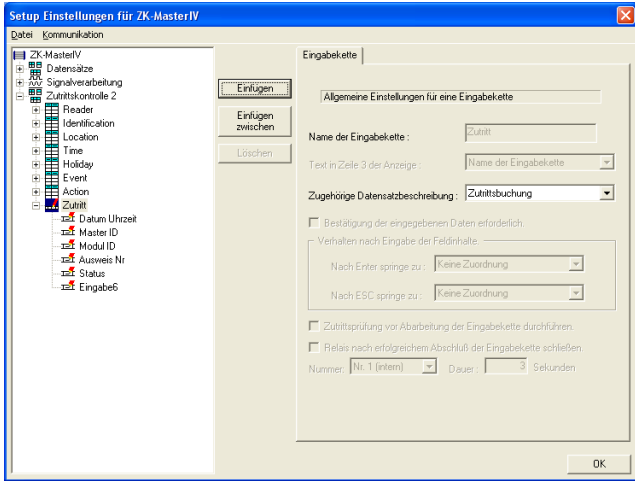
After creating an input chain and setting a designator, it has to be assigned to a data record. This is done via the field with the appropriate data record description.

If no assignment is defined at this point, no data record is created. It is reasonable, if the input chain is only used for defining a GV (as explained in chapter 5.2.2).

Figure 121: Creating input chains

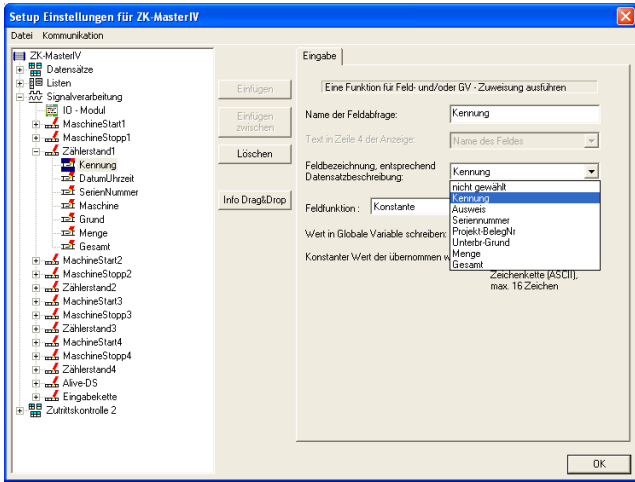
### 5.2.6.2 Defining input fields

**Note:**  
All inputs always apply to the input field selected in the tree structure.



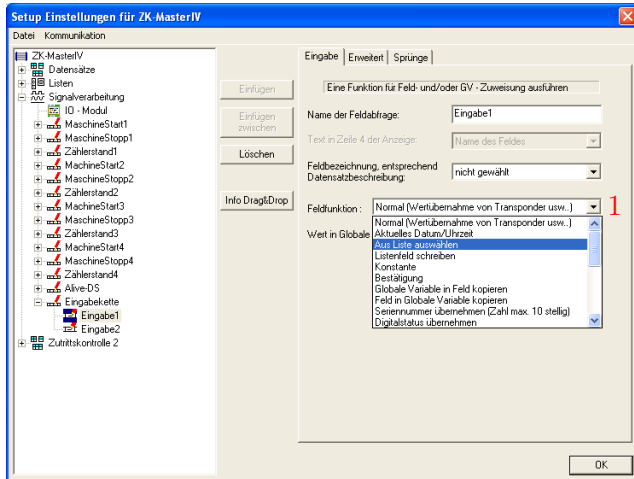
After adding the input chain fields by pasting the input chain, these input chain fields can be configured. Paste the input chain fields

Figure 122: Add input fields



A data record description is assigned to the input chain (to save the data). You have to assign the input chain fields to the appropriate field of the data record description analogously. Data type and size of the data, that shall be processed, is set via this assignment.

Figure 123: Configuration of the input chain fields of the access control



At next you have to assign the collection function for data to the input chain field. Via this functions you set, which data (in which form) are transmitted to the field.

Figure 124: Assignment of the collection function to an input chain field of the access control

The following input functions (1) are available:

### 5.2.6.2.1 Field functions in general

- ▶ Normal = Input via keyboard, bar code, transponder or smart card.
- ▶ Select from list = In order to do this an assignment to a defined list has to occur. You may find a detailed description in chapter 5.2.5.
- ▶ Write list field = The value of a GV can be written on a selected list field via this function.
- ▶ Constant = The field is filled with a constant value.
- ▶ Copy global variable to field = The value of the current global variable is copied into this field.
- ▶ Apply serial number (10-digit number)
- ▶ Apply digital measurement (16-digit number)
- ▶ Apply counter reading
- ▶ Apply function value
- ▶ Apply threshold status
- ▶ Apply GPRS Alive counter
- ▶ Apply firmware version (xx.xx.xx.xx)
- ▶ Apply status of summer-/wintertime (S/W)
- ▶ Apply GPS data (27-digit RMC)
- ▶ Apply GPS data (variable selection)
- ▶ Copy Timeboy variable to field
- ▶ Start/Stop Timer

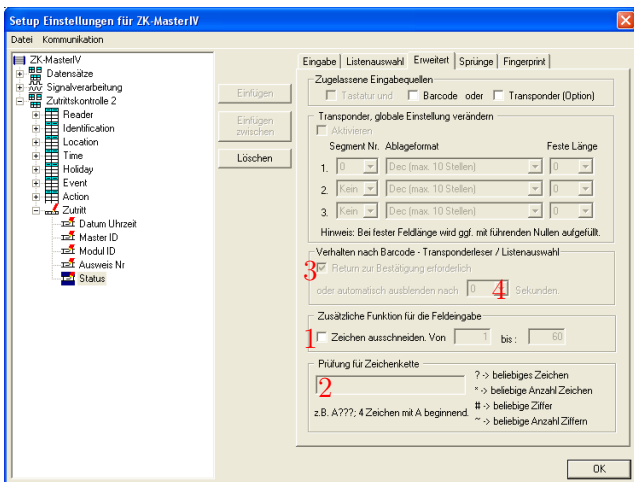
- ▶ Carry out access control with GV = You can carry out an access control within an input chain.
- ▶ Switch relay
- ▶ Apply debug value

5.2.6.2.2 Field functions of the access control

- ▶ Access: apply ZM (AccessMaster) = The value of the ZM is applied from the reader list.
- ▶ Access: apply TM (DoorrModule) = The value of the TM is applied from the reader list.
- ▶ Access: Apply card number = The read card number is applied.
- ▶ Access: Apply status = The basic status of the initialized ZK-bus and of an action carried out is applied

5.2.6.3 Expanded

You can use the cutting of the field values and the check against a reference string as expanded configuration. Further options are not available.



On the register card Expanded the option Cut out character of (1) is activated and the field part is set by setting start and end position of the fields to be read. Additionally a format check for string (2) (with a set format) can be carried out here.

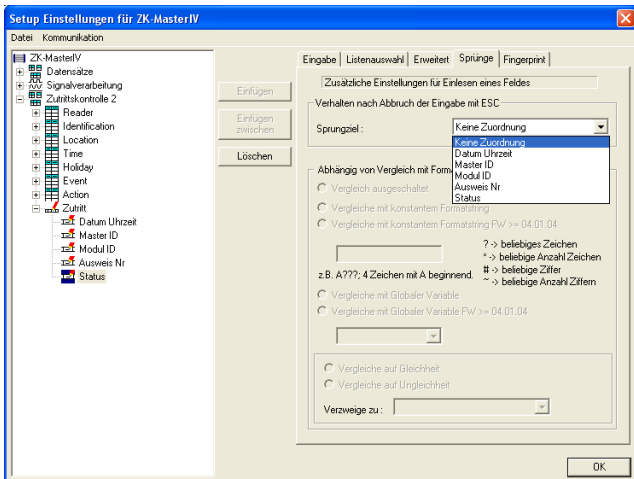
Figure 125: Expanded

### 5.2.6.4 Reaction on list selection

- ▶ If you tick off Return necessary for confirmation (...), the list is displayed until a selection is made (in case of a list selection).
- ▶ (no tick) Timeout 0 (...). The first found list input is applied without being displayed. Please be careful in this case!
- ▶ (no tick) Timeout >0. The list is displayed. You can select a list input by scrolling and apply it via ENTER. If no acceptance occurs via ENTER, the selected list input is applied automatically after the set time.

### 5.2.6.5 Jumps

This field is available, if one of the following input functions is selected: Normal, Select from list, Write list field, Confirmation, Copy GV/Timeboy variable to field, Copy field to GV/Timeboy variable, Fingerprint: scan/ teach-in fingers/ delete finger templates/ carry out identification/ carry out verification or apply debug value.




You can define jump targets within the input chain for ESC or depending on a check (if this function is available). That way it is possible e.g. to check a status value (0/1). If the desired value is not available, you can leave the input chain and avoid the unwanted creation of a data record that way.

Figure 126: Defining jumps

### 5.2.7 Signal processing

Via the signal processing the digital and the analogous inputs are supervised and the digital outputs controlled.

#### 5.2.7.1 Use as Start/Stop



**Note:**  
 In principle it is valid:  
 The digital input 1 can be used with at most 1 kHz; the input 2 with at most 10 Hz.

When using as Start/ Stop a single digital input is allocated. It is appropriate to use the slower 10 Hz input for this.

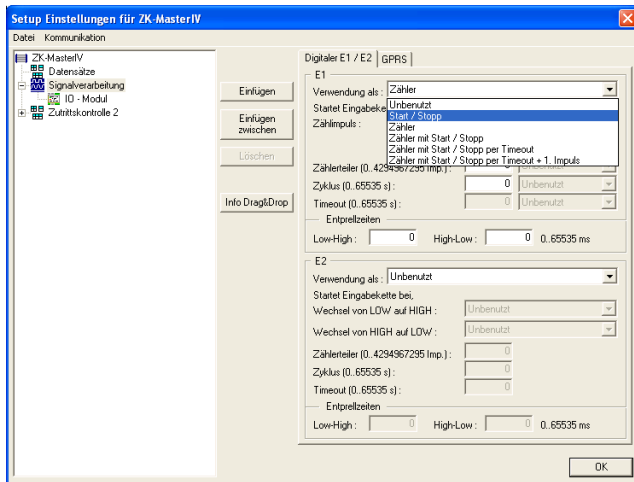


Figure 127: Use as Start/Stop

When using as Start/ Stop an edge change (High to Low or Low to High) is interpreted as a valid signal, only if the signal level is over the period of time set as debounce time. Then the assigned input chain is started once only. This function you can use e.g. to supervise a machine. E.g. edge change from Low to High: The input chain Production could be called up once only. Edge change from High to Low: The input chain Interruption would be started.

The cycle indicates the interval, in which a data record is created (irrespective of an impulse). The input chain, selected in the started/stopped machine is carried out cyclically.

### 5.2.7.2 Use as counter

When using as counter a single digital input is allocated. It is reasonable to use the faster 1 kHz input for this. For this please note the following:

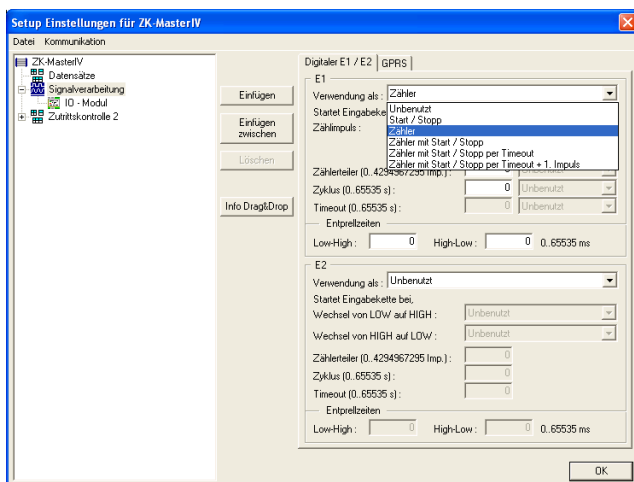


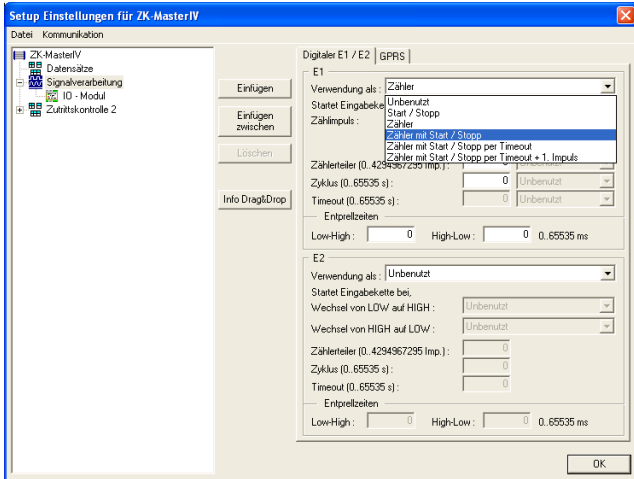
Figure 128: Use as counter

A valid counting impulse starts the assigned input chain. The counter splitter indicates, how many single impulses can be combined into one counting impulse. This value can be between 0 and 4.294.967.295. The cycle indicates the interval, in which a data record is created (irrespective of an impulse).



### 5.2.7.3 Use as counter with Start/Stop

When using as counter with Start/Stop two digital inputs are allocated. The faster 1 kHz input is used as counter and the slower 10 Hz input as Start/Stop.

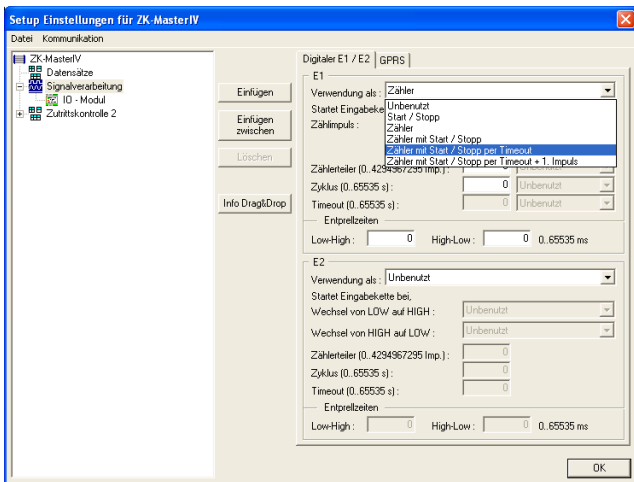


Both inputs are configured according to their use (see figure 128 and 127. Here you also have to pay attention to the debounce time for a defined signal level.

Figure 129: Use as counter with Start/Stop

### 5.2.7.4 Use as counter with Start/Stop via timeout

When using as counter with Start/Stop via timeout a single digital input is allocated. It is reasonable to use the faster 1 kHz input for this, because it also functions as counter.



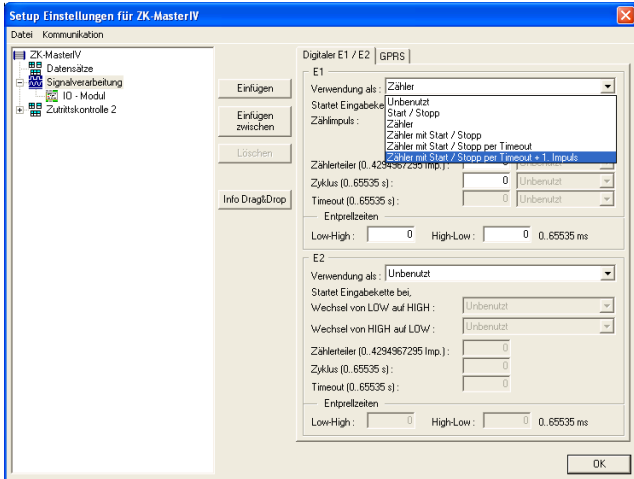
The counter for produced pieces is the signal for a running machine concurrently. In order to notice interruption or switching-off of the machine the timeout is supervised. When the timeout has run out without registering a counting impulse, an interruption data record is created. The timeout is put back after each impulse (change from Low to High), that fulfils the conditions of the debounce time.

Figure 130: Use as counter with Start/Stop via timeout

The cycle indicates the interval, in which a data record is created (irrespective of an impulse). It is activated after the first impulse and deactivated after reached timeout. The cycle carries out the input chain for Start and counting impulse.

5.2.7.5 Use as counter with Start/Stop via timeout and 1st counting impulse

When using as counter with Start/Stop via timeout and 1st counting impulse a single digital input is allocated. It is reasonable to use the faster 1 kHz input for this, because it also functions as counter. Furthermore it is possible to create a data record with the first counting impulse.



The input chain, assigned to first impulse and counting impulse, is started with the first impulse (change from Low to High) and then according to the counter splitter. The counter splitter indicates, how many impulses are necessary to activate the assigned input chain. The input chain is not carried out, if 0 is indicated.

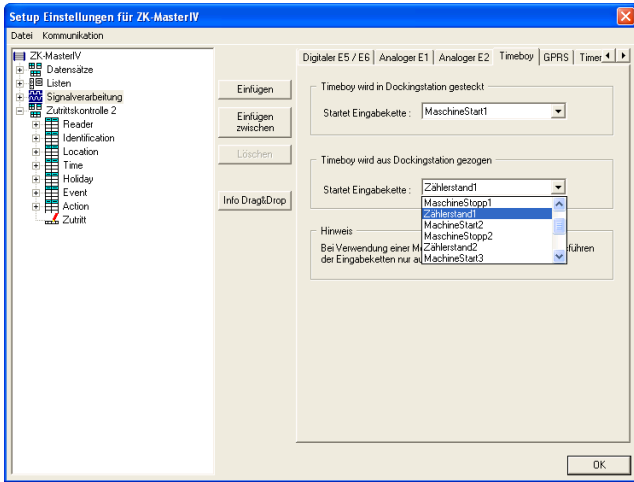
If no further impulse is detected within the time of the timeout, the input chain for the timeout is started. A further impulse restarts the input chain of the 1st impulse.

Figure 131: Use as counter with Start/Stop via timeout and 1st counting impulse

The debounce time indicates, how long the signal level has to remain unchanged to be detected as impulse. This is valid for both the change of level from Low to High (starting a device) and the change of level from High to Low (stopping a device).

The cycle indicates the interval, in which a data record is created (irrespective of an impulse ). When stopping the machine the cycle is deactivated (as far as the machine status is Start).

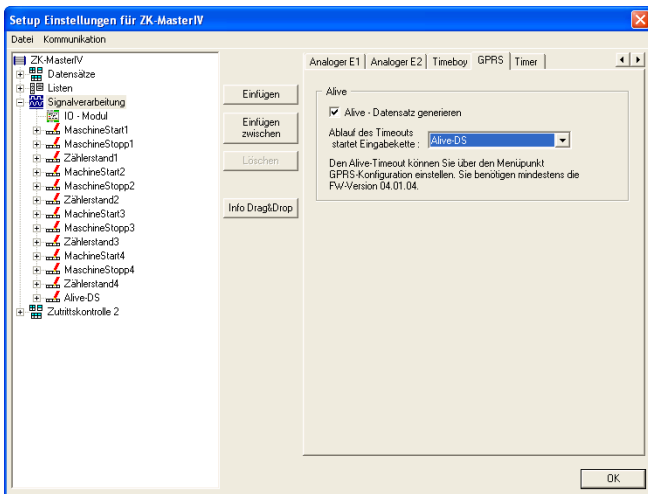
### 5.2.7.6 Connection Timeboy



Via the register card Timeboy input chains can be assigned to the actions Plug-in Timeboy and Pull-out Timeboy. They are activated, when the action occurs.

Figure 132: Assignment of input chains to plugging-in- and pulling-out-events

### 5.2.7.7 Alive data record



With elder firmware versions the alive data record was created via the F6 input chain.

Now it is possible to create an input chain for the creation of alive data records via signal processing. In both variants the alive parameter in the GPRS.ini has to have a value larger than 60.

The ZK-MasterIV checks Alive via F6 chain and then Alive via signal processing.

Figure 133: Setting the alive data record

### 5.2.7.8 Setting of timers

### 5.2.7.9 Setting of timers

## 5.2.8 Mathematical operations

The mathematical operator can carry out addition, subtraction, comparison (equal, not equal, greater/less than) and negation (No). The operand (the information) has to be available as string in decimal form

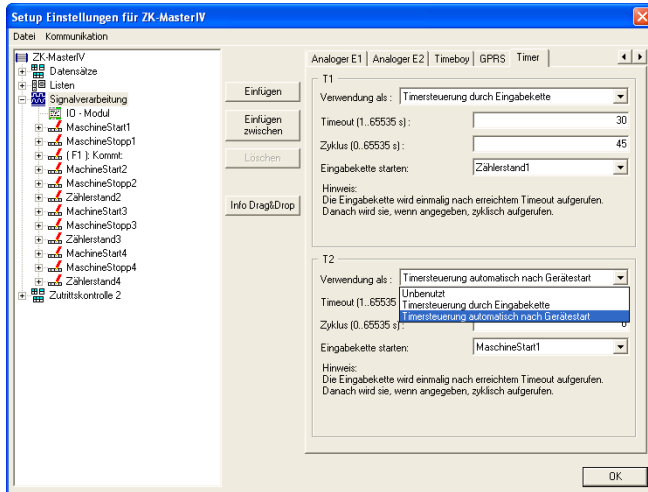


Figure 134: Setting of timers

Two types of timers are available. They are started either via an input chain (call up the function Start/stop timer) or automatically after starting the ZK-MasterIV. An input chain can be assigned to each timer. It is called up after the timeout was reached and then, if set, cyclically.

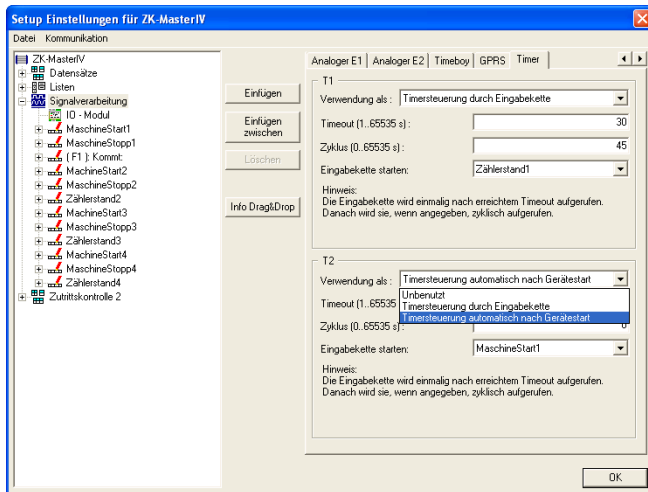


Figure 135: Setting of timers

Two types of timers are available. They are started either via an input chain (call up the function Start/stop timer) or automatically after starting the ZK-MasterIV. An input chain can be assigned to each timer. It is called up after the timeout was reached and then, if set, cyclically.

[0..9]. The operands can be provided as constants, global variables or fields with the format (only numeric characters).

The operations addition and subtraction do not have to be explained further.

The following is valid for the negation (No): Each value of the operand  $> 0$  has the result = 0; each value of the operand = 0 has the result = 1.

The following is valid for the comparison operations: A positive comparison (Yes) has the result = 1; a negative comparison (No) has the result = 0.

The result is stored in a global variable. The value this GV can be used for the decision for jump target.

### formatting operations

Record fields and GV (global variables) can be convert between hexadecimal strings and dezimal strings or between dezimal strings and hexadecimal strings. You can set a mask of zero sign to get a constant length of string. The maximum mask length is 16 characters. The max. resolution of operands is 8 Byte (64bit).

### Example

Value in GV 0000290A should be convert to a dezimal value 9994 with a mask of 00000000. The result is 00009994.

## 5.3 Creating setups

### 5.3.1 Setup for access control version II

In this chapter there is explained, how to create the setup for access control and how to transmit all necessary information to the device. You want to use the example of chapter 3.6.4 and complete it with this setup. That way you can comprehend and test the example continuously. Please plan 3 up to 4 hours for working through this chapter (incl. hardware installation). Take the time so that you can comprehend each step in a test environment.

#### 5.3.1.1 General

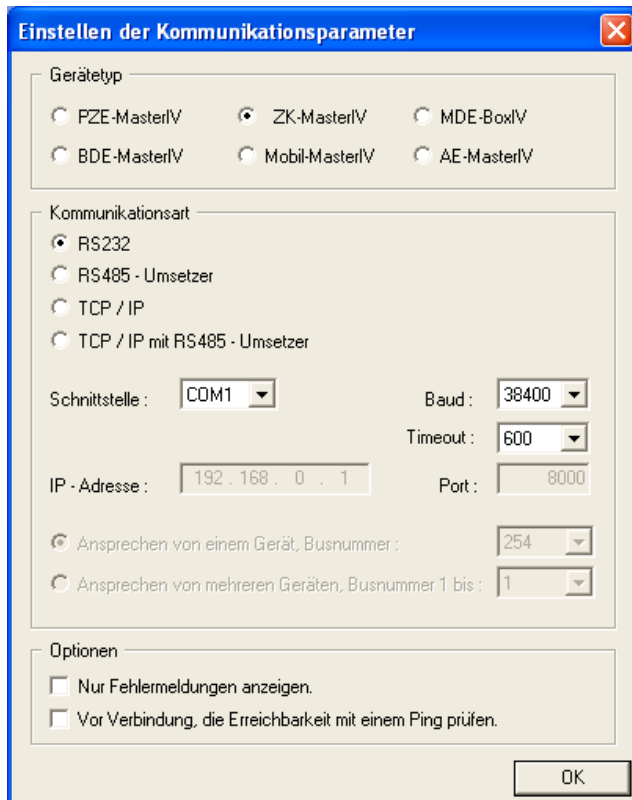
There are the following special features for a setup of access control. The ZK-MasterIV does not have a keyboard or a display. Therefore operating via direct user input on terminal is impossible.

#### 5.3.1.2 Hardware components of access control system

In order to carry out an access control you need the hardware components, wired according to the instructions (see figure 52), as explained in chapter 3.6.4.

### 5.3.1.3 Basic settings

At first you start the DatafoxStudioIV. Then you have to open the dialogue for setting the communication parameters via *< Kommunikation => Einstellungen >*.



Set ZK-MasterIV as device type.

In this example you select the communication type RS232. Select the interface, as it is allocated on your server (COM1 by default). Baud rate and timeout value can remain on the default values in this case. But you should check the concurrence of the settings via the system menu-BIOS of the ZK-MasterIV. If they are not concurrent, you have to adapt the parameters via terminal or DatafoxStudioIV. Confirm all changes via OK.

Figure 136: Setting of the device type and the communication parameters

This setup (standard AESetup1) you can save with an own name via *< Datei => Speichern unter >*. In our example you use the name ZK-MasterIV-Setup.aes. You can also create a new setup file via *< Datei- > Neu >* and save it with an own name. The setting of device type and communication parameters is important.

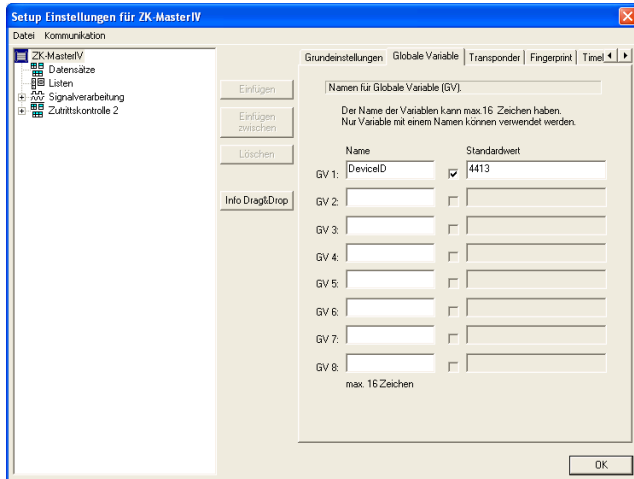


Figure 137: Definition of global variables

In order to demonstrate the use of global variables you define a global variables named DeviceID. It is preallocated with the default value 4413. Each data record is characterized with this variable. If several terminals are used, data can be filtered and evaluated that way. In addition you define two global variables named Entry (default value 1) and Exit (default value 2). Later this two values are used for a list selection to collect the reasons clocking-on and clocking-off automatically.

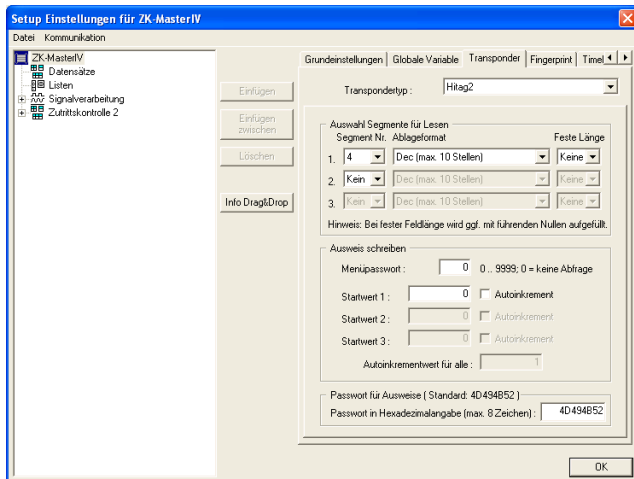


Figure 138: Setting of the transponder type

In this example the transponder type Hitag2 is used. In order to read the card number the segment 4 is used with the filing format decimal (at most 10 digits).

### 5.3.1.4 Creating a data record description

In order to create a data record description you should exactly know which data have to be created.

Example: While a ZK-booking a data record should be created, containing the following information:

- 1.) **Datum\_Uhrzeit** (indicates, when a query for access authorization was run)
- 2.) **Master\_ID** (contains the device-no. of the access master)
- 3.) **Modul\_ID** (contains the device-no. of the TS TMR33-module, the query was run for)
- 4.) **Ausweis\_Nr** (read card number)
- 5.) **Status** (contains the status of the access control)

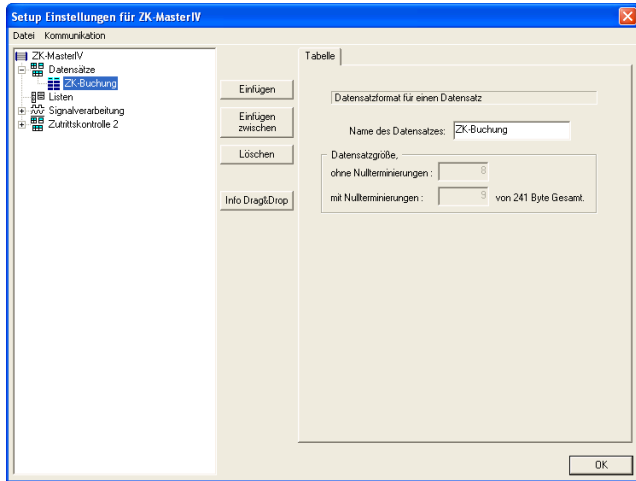


Figure 139: Creation of a data record description

The dialogue for editing the setup is opened via a double click on the client range of the DatafoxStudioIV or via `< Setup => Editieren >`. Mark the input Data records on the left side of the tree and then click on Paste. Under Data records an entry Datensatz1 is created. Mark this entry and you can edit its characteristics on the right side. Please enter the name ZK-booking there and mark the entry again in the tree. Now the name is updated.

Now click on the button Paste six times to create the 6 data fields. The rough definition is finished. Now you have to set which data types (and their length) should be in each field. The following data types are available: string with numeric characters, string with ASCII-characters (text) and date\_time.

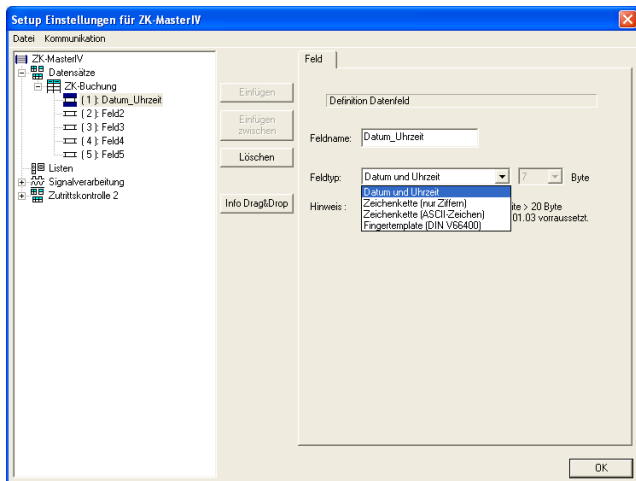


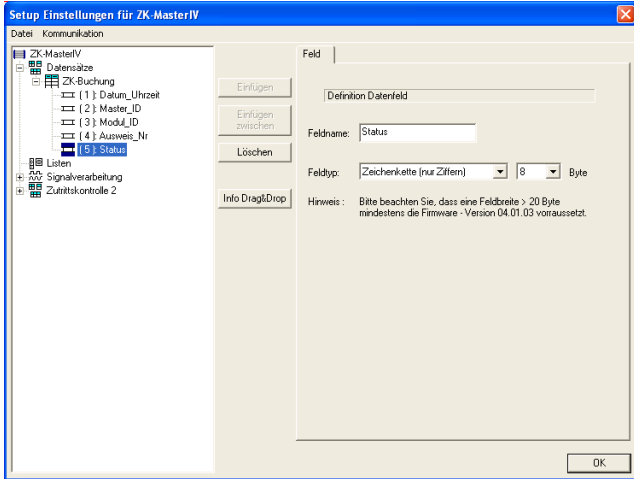
Figure 140: Setting of the data type

Mark an input in the tree and set the characteristics on the right side. Date\_Time is set as date\_time. Master\_ID and Module\_ID are set as string with numeric characters (length 8). Because you know that a Hitag2 transponder is used the Card is defined as string with numeric characters (length 4). The Status is set as string with ASCII-characters (length 8).

### 5.3.1.5 Creating the access control lists

According to the hardware configuration of the example in chapter 3.6.4 the access control lists have to be created as \*.txt files with the following name and content. Lines starting with a semicolon are comment lines and will help you to understand better. You can use a simple ASCII-editor (e.g. Microsoft Editor or WordPad) to create the text files. Save these files and the setup file in the same directory. That way assigning the right files is eased, when you work with several setups.





After setting all characteristics of the fields, the tree looks like that.

Figure 141: Complete data record description

**Reader-List (Reader.txt)**

```

;ID ZM TM RefLocation RefAction PinGeneral
1 1 320 0 0 0
2 1 000 1 1 0
3 1 010 2 0 0
4 1 011 2 2 0
    
```

**Identification-List (Identification.txt)**

```

;ID Group Pin Menace ActiveStart ActiveEnd ActiveGeneral
1111 1 1111 911 2005-01-01 2008-01-01 1
2222 2 2222 922 2005-01-01 2008-01-01 1
    
```

Set the Identification list to the columns ID, Pin and Menace according to your cards. The other settings are applied.

**Location-List (Location.txt)**

```

;ID RefGroup RefTime RefTimeNoPin
1 1 3 3
1 2 3 3
2 1 1 0
    
```

**Time-List (Time.txt)**

```

;ID Weekdays TimeStart TimeEnd
1 12345 07:00 13:00
2 12345 13:01 18:59
3 12345 07:00 18:59
    
```

Action-List (Action.txt)

;ID	RefReader	PortOut	Elapse	RefTime
1	1	1	25	0
1	2	2	25	0
2	3	1	25	0
2	3	2	25	0

Create the event list (Event.txt) and the holiday list (Holiday.txt) as empty files. In the following example they are not necessary.

You may find a detailed description of the single lists and the connections of data records in chapter 3.6.4.

5.3.1.6 Creating an input chain of access control

There is no keyboard or display on the ZK-MasterIV. Therefore operating by direct user input is not possible. The input chain, you want to create, will carry out the control (whether a person is access authorized or not). Interaction with the user is limited to the card held in front of the reading device of the system. Depending on the control result a relay or open-collector is switched or not. A data record (with a status message) is created at any rate. That way you can comprehend, who tried to enter this area.

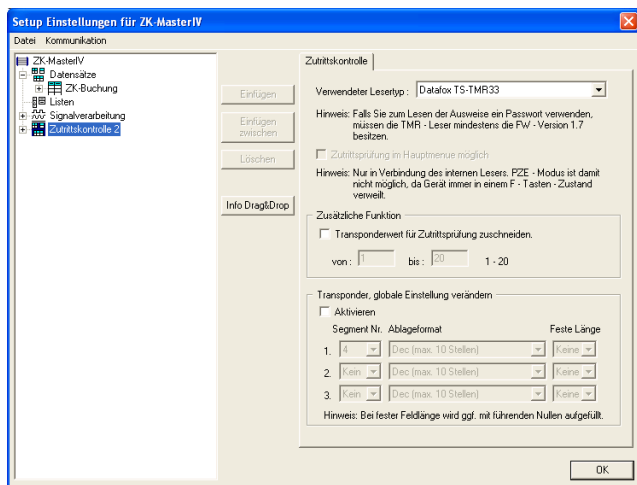
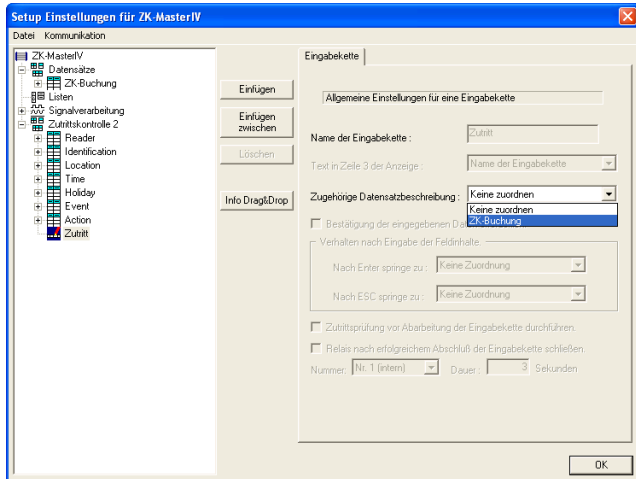


Figure 142: Settings of the access control 2

At first you control the settings for the access control. Mark the input Access control2 on the left side of the tree. There Datafox TS TMR33 should be selected as used reader type.

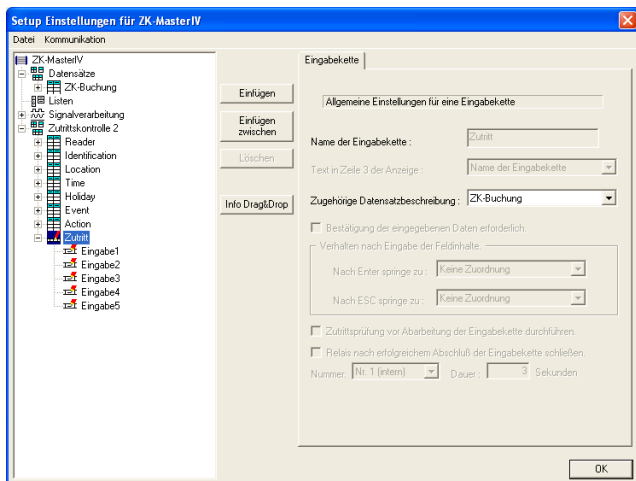
In this example you do not need the option Cut transponder value for access control.

The settings of the global transponder remain also unchanged.



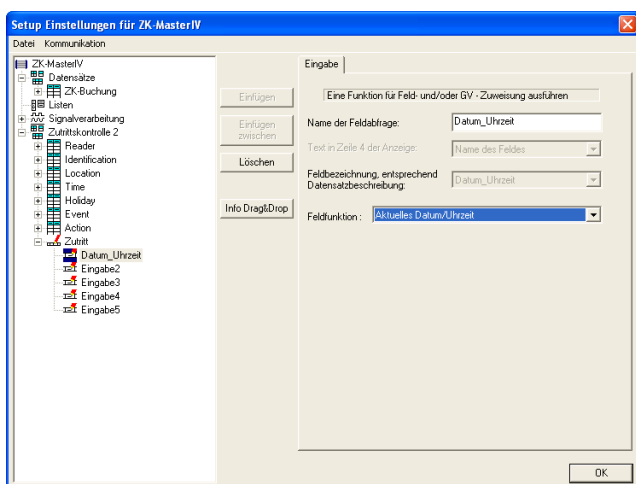
The next step is to assign an appropriate data record description to the input chain (for saving the booking data).

Figure 143: Assignment of the data record description



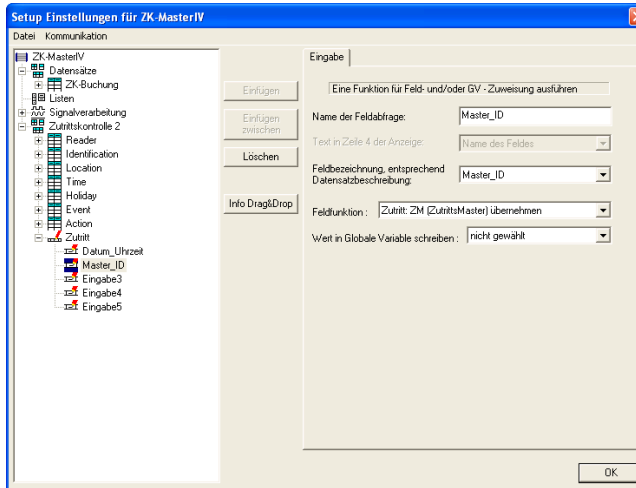
Erstellen Sie fünf Eingabekettenfelder innerhalb der Eingabekette für die Zutrittskontrolle.

Figure 144: Creating the input chain



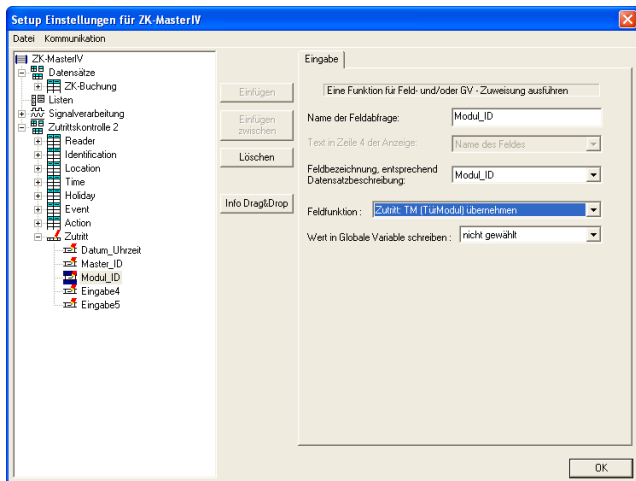
Now you set the characteristics of the input chain fields. For Name you use the designation you already used in the data record description. Then assign the appropriate field of the data record description. In our case it is Date\_Time. A function is not necessary here, because format and value are set by the system.

Figure 145: Definition of the input chain field Date\_Time



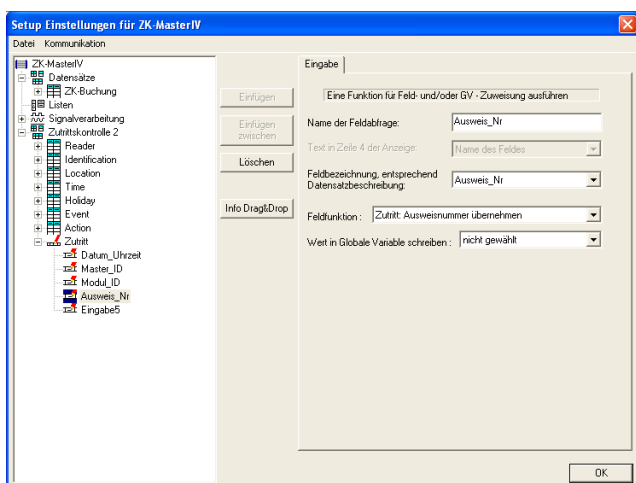
This input chain field is named Master\_ID. Assign the same-named field to the data record description. Select the function Access: apply ZM (AccessMaster).

Figure 146: Definition of the input chain field Master\_ID



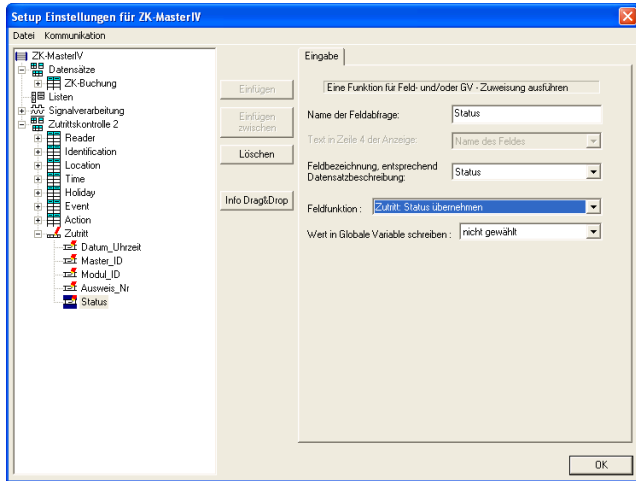
This input chain field is named Module\_ID. Assign the same-named field to the data record description. Select the function Access: apply TM (DoorModule).

Figure 147: Definition of the input chain field Modul\_ID



This input chain field is named Card\_No. Assign the same-named field to the data record description. Select the function Access: apply card number. The settings on the register cards Expanded and Jumps are not changed.

Figure 148: Definition of the input chain field Card\_No



This input chain field is named Status. Assign the same-named field to the data record description. Select the function Access: apply status. The settings on the register cards Expanded and Jumps are not changed.

Figure 149: Definition of the input chain field Status

### 5.3.1.7 Transmission of the complete configuration to the terminal

When you have worked through all the steps, the setup is finished now. In order to check the booking records the setup and the lists have to be transmitted to the terminal (ZK-MasterIV).

Connect the ZK-MasterIV to the PC according to the selected communication type (see figure 141). Make sure that the PC interface is configured correctly, e.g. the baud rate, number of data bits, parity and stop bits of the COM-interface have to be concurrent to the configuration of the terminal.

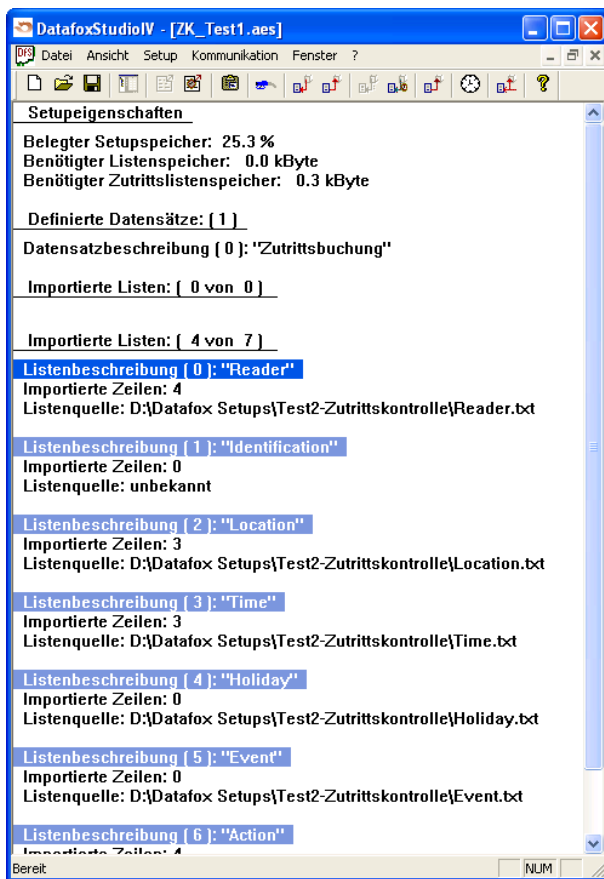
Connect the terminal to the voltage source. Within the booting process a connected RS485-bus (incl. RS232 branch line) is scanned for available modules. If the access components are connected correctly (according to figure Abbildung 52 it is indicated by a short flash of all LEDs (ca. 1s) in connection with a signal of the buzzer (ca. 1s). You may find further status signals via the LEDs in table 23.

In both cases you can transmit a new setup to the device via the DatafoxStudioIV.



yellow	green	red	state of the TS TMR33-xx
off	off	off	No supply voltage is connected
on	off	off	Supply voltage is connected
on	on (ca. 1 s)	an (ca. 1 s)	Acoustic signal by buzzer (ca. 1s) signalizes module test
on	off	off	Status after module test = Status OK
on	off	on (ca. 10 s)	Lists of the access master are updated
on	off	on (duration)	Configuration error via access lists (check of status signals necessary.))
flash	off	off	Signalizes readable card in field
on	on (ca. 1 s)	off	Read card is access authorized, in addition acoustic signal by buzzer (ca. 1s)
on	off	on (ca. 1 s)	Read card is not access authorized
on	flash	off	PIN input awaited

Table 23: Status display of the access components via LEDs



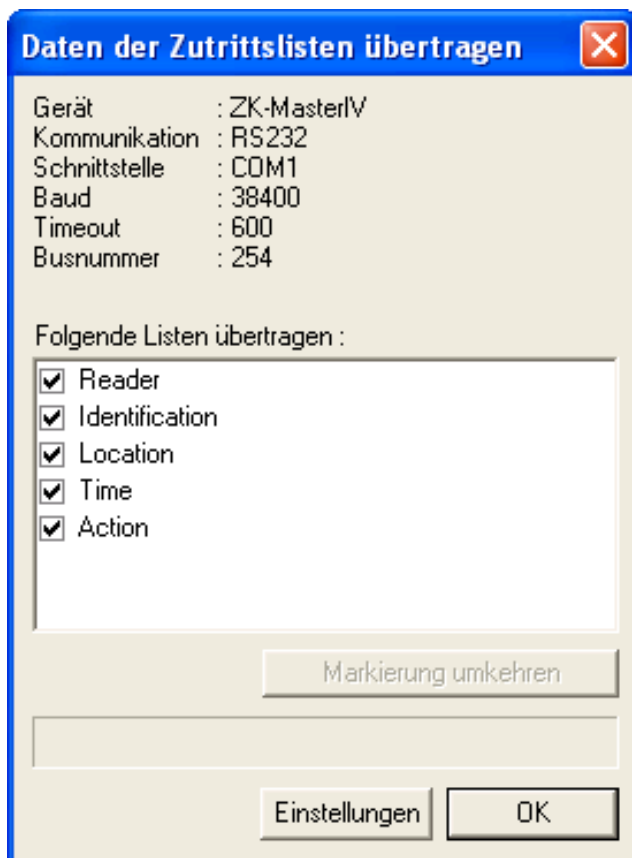
Import the access control lists (created in chapter 5.3.1.5) to the setup via `< Setup => Zutrittskontrolllisten importieren >`. If the import is successful, the file path is displayed as list source.

Figure 150: Import of the access control lists



Now you can transmit the setup to the device via *< Kommunikation => Setup schreiben >*. The progress bar indicates, that data are transmitted to the device. A successful conclusion of the transmission is indicated by a message you have to confirm via OK.

Figure 151: Transmitting the setup to the device



At last you can transmit the access control lists to the device via *< Kommunikation => Zutrittskontrolllisten laden >*. In addition you can set there, which lists shall be transmitted. The progress bar indicates, that data are transmitted to the device. A successful conclusion of the transmission is indicated by a message you have to confirm via OK. For ca. 10s both the red and the yellow LED are flashing. This indicates, that the access control lists on the terminal were updated.

Figure 152: Transmitting the access control lists to the device

All red LEDs should turn out then. If they do not, you should check the list contents, especially the Bus-No. (DM) of the reader list and the configuration of the access components via the dip switch. If everything is okay, you can test the access control system.