

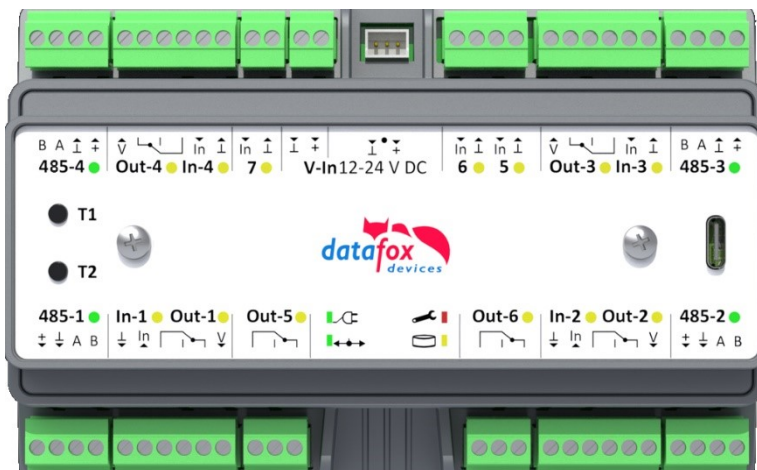


Datafox GmbH • Dermbacher Straße 12-14 • D-36419 Geisa • www.datafox.de

Manual

Datafox KYO Fourloc

Flexible data collection with method



© 2023 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 license or the use of the soft- and hardware. Copies of the floppy disks 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.

Alterations

Alternation in this Dokument

Date	Chapter	Discription
4.12.2023	all	Revision the manual to new version 04.03.21.xx

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 genera- tion	YY. Compatibility (which versions can be used to- gether)	ZZ. Version number (functional exten- sion)	Build Troubleshooting (with a new version the Build number is reset)
z. B. AE-MasterIV	04.	03.	9.	04

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.

Firmware StudioIV and DLL validity

Firmware: 4.03.21.xx.

Studio: 4.03.21.xx

DII: 4.03.21.xx

The DatafoxStudioIV is backward compatible. This means that you can configure a device with a newer DatafoxStudioIV also older firmware, the device only supports the natural functions that are implemented in the older firmware version. I.e., relevant to the functions that are possible, is always the manual state that the firmware associated with the Setup equivalent. It is not possible to provide a centering firmware configured with a stand of DatafoxStudioIV to who is older than the firmware. recommendation:

If possible, use always the current version of DatafoxStudioIV.

What features are supported in which software versions, is from the file:

Datafox MasterIV, SW version xxx.pdf list as shown.

The file is located on the Datafox DVD and for download on the homepage. Please also note the instructions in each chapter in the manual. The updates are available on our website under www.datafox.de download.

Inhalt

1.	For your Safety	1
2.	Introduction	2
2.1.	Structure of the Documentation	2
2.2.	Guarantee Restriction	2
2.3.	Typography of the Documentation	3
2.4.	Important General Notes	3
3.	Intended Use and Environmental Protection	5
3.1.	Regulations and Notices	5
3.2.	Power supply	5
3.3.	Environmental Influences	5
3.4.	Mounting outdoors	6
3.5.	Temperature	7
3.6.	Repair	7
3.7.	Cleaning	8
3.8.	Further Notices	8
3.9.	Disposal	9
4.	System Requirements / Hardware	10
4.1.	System Structure	10
4.2.	Installation requirements for Operating Datafox Devices	11
4.3.	General Hardware Information	12
4.3.1.	Hardware equipment	12
4.3.2.	Behavior in case of power failure	12
4.3.3.	UPS	12
4.4.	Compatibility	13
4.4.1.	Firmware File Archive (*.dfz)	13
4.4.2.	Datafox Devices and Device Firmware	13
4.4.3.	Device Firmware and Device Setup	14
4.4.4.	Device Firmware and Communication DLL	14
4.4.5.	Communications DLL and DatafoxStudioIV	14
4.4.6.	DatafoxStudioIV and Device Setup	14
4.4.7.	Update / Downgrade	15
5.	Device	16
5.1.	Commissioning	16
5.2.	Guideline for Commissioning	17
5.2.1.	Set-up of the device	17
5.2.2.	Installation of the device	17
5.2.3.	Troubleshooting during Commissioning	17
5.3.	Communication of Hardware V4 Devices	18
5.3.1.	Communication via USB	18
5.3.1.1.	Automatic detected connected USB to PC	19
5.3.1.2.	Installing USB driver for Hardware V4 Devices	20
5.3.2.	Communication via TCP / IP	21
5.3.2.1.	Communication TCP / IP via network-cable	22
5.3.3.	Communication TCP / IP via wLAN / Wifi	22
5.3.3.1.	M111_WLAN ESP32-c3 ML01 (wLAN-Modul DF-WL03)	24
5.3.3.2.	Texas Instruments TI-CC3135 (Generation 2)	25
5.3.3.3.	Redpine (Generation 1)	26
5.3.3.4.	Connection of the Terminals via TCP/IP DNS / DHCP	28
5.4.	Operation with Box-Devices V4	30
5.4.1.	Bios Menu of Box Devices V4	30
5.4.2.	Anzeige der Status LEDs beim Fourloc	33

5.5.	Mounting of the Fourloc	34
5.5.1.	Mounting on a hat-rail	34
5.6.	Connecting of the KYO Fourloc	35
5.6.1.	Connctors of the KYO Fourloc	35
5.6.2.	Power supply for the KYO Fourloc	36
5.6.3.	Power via POE	37
5.7.	Connection and wiring of the access control	38
5.7.1.	Configuration and structure of the Access control	38
5.7.2.	Description of Tables for Access Control 2	41
5.7.3.	Wiring variants for the KYO Fourloc.....	44
5.7.3.1.	Wiring in a star form of the access control for the KYO Fourloc	44
5.7.3.2.	Two doors, 4 access-reader	48
1.1.1.1	Cable plan for KYO-Oneloc and Intera 2 access reader.....	50
5.7.4.	Instructions for the electrician for installing the access control system	51
5.7.4.1.	Star-shaped bus wiring	51
5.7.5.	Access-control with Intera 2.....	53
5.7.5.1.	EVO Intera II, Individual settings.....	56
5.7.5.2.	Functionality of the EVO Intera II	56
5.7.5.3.	Global function.....	57
5.7.5.4.	Einstellung der Gerätefunktionen.....	57
5.7.5.5.	Settings for standby	59
5.7.5.6.	Setting for standard operation.....	59
5.7.5.7.	Preview of reader behavior	60
5.7.5.8.	Transfer to the device	60
5.7.6.	Access control II with EVO Agera	61
5.7.6.1.	Display and operation	61
5.7.6.2.	Display for state of access control	62
5.7.6.3.	Display the number keypad	62
5.7.6.4.	Error message	62
5.7.6.5.	Bios-menu	63
5.7.6.6.	General configuration	63
5.7.6.7.	Display configuration	64
5.7.6.8.	Bus configuration	64
5.7.6.9.	Setting the bus address of the reader for RS485 bus.....	64
5.7.6.10.	Activate the termination resistor of the bus	64
5.7.7.	Function extention for access control II.....	65
5.7.7.1.	General description.....	65
5.7.7.2.	Examples.....	66
5.7.7.3.	Description of the table „Action2“	70
5.7.7.4.	Additional functions for Access Control.....	71
5.7.7.5.	List Presence	72
5.7.8.	Integration of a Burglar Detection System (BDS)	73
5.7.8.1.	Configuring up the BDS	73
5.7.8.2.	Relays and digital inputs for controlling the BDS (Type 2).....	74
5.7.8.3.	Assigning codes for arming and disarming (Type 3)	75
5.7.8.4.	Associating BDS sections to readers (Type 4).....	76
5.7.8.5.	Privileging transponders to control the BDS.....	77
5.7.8.6.	Statuscodes.....	78
5.7.8.7.	Pre-checked online processing graph	79
5.7.8.8.	Example for the BDS integration.....	80
5.7.9.	Automatic relay release upon opening of the door	81
5.7.9.1.	Supervised doors.....	81
5.7.9.2.	Configuration	82
5.7.9.3.	Requirements for the ReaderProps entry.....	82
5.7.9.4.	Logical conditions implemented by the access controller	82
5.7.9.5.	Special case: Relays operated by time model.....	83

5.7.9.6.	Configuration sample	83
5.7.9.7.	Access control lists	83
5.7.9.8.	Additional lists.....	84
5.7.10.	Calculation for the power supply of Access modules	85
5.7.11.	Cable length and cable cross section for access wiring	86
5.7.12.	Status messages of the access control.....	87
5.7.13.	State signals of reader modules via LEDs.....	92
5.7.14.	Online functions for the access control	93
5.7.14.1.	Online via http-protocol	93
5.7.14.2.	Online via DLL connection	96
5.7.15.	Function for access control U&Z (locking cylinders).....	97
5.7.15.1.	Design example	97
5.7.15.2.	First start with locking cylinders	100
5.7.15.3.	Assembly and disassembly of the cylinders	100
5.7.15.4.	Set up the wireless network for cylinder.....	101
5.7.15.5.	Battery state and live time.....	102
5.7.15.6.	Change the access control master ID and knob Active Time	103
5.7.15.7.	Optical and acoustic signals of the U&Z locking cylinder.....	104
5.7.15.8.	Optical and acoustic signals of the U&Z door handle	105
5.7.15.9.	Resetting the U&Z locking cylinder	105
5.7.15.10.	Supported transponder technologies	106
1.1.1.2	Service key broken / lost.....	107
1.1.1.3	Replace service key.....	107
1.1.1.4	Technical data of the radio module	107
5.7.16.	Office mode using Uhlmann&Zacher radio locks.....	108
5.7.17.	Office mode implementation (Variant 1 – Secure Method).....	108
5.7.17.1.	Activating office mode.....	108
5.7.17.2.	Operation in office mode.....	108
5.7.17.3.	Revoking office mode	109
5.7.17.4.	Summary	109
5.7.18.	Office mode implementation (Variant 2 – Classic Method).....	109
5.7.18.1.	Office mode in classic mode	109
5.7.18.2.	Configuring classic office mode	110
5.7.18.3.	LED and Buzzer feedback in classic office mode.....	110
5.7.19.	Operation / activation-deactivation the Office-Mode.....	111
5.7.19.1.	activation	111
5.7.19.2.	deactivation	111
5.7.19.3.	Remarks	112
5.8.	Data on Card	113
5.8.1.	General infomations.....	113
5.8.2.	Settings for using DataOnCard	114
5.8.3.	DataOnCard on the access control reader.....	118
5.8.4.	DataOnCard and a access control reader - wiring.....	119
6.	technical data KYO Fourloc	120
7.	Index	121

1. For your Safety

Safety Information for Datafox Products



The KYO Fourloc must only be operated according to the instructions given in the manual. Do not insert any foreign objects into the openings and ports. The device must not be opened. All maintenance work must only be performed by authorized specialists.



Some devices contain a lithium ion battery or a lithium battery. Do not throw into fire!

Supply voltage: 12 Volt DC
See respective type label / technical data.
The device must only be operated with a power-limited power supply according to EN 60950-1. If you do not observe these instructions, the device may be damaged.

Attention!

The following temperature ranges must be observed
Working area / storage temperature: -20° C bis +70° C
Mobile communications module: -20° C bis +55° C



In areas with cellphone ban, GPRS, WLAN and other cellular modems must be turned off.
Persons with heart pacemakers:
When using the device, maintain a distance of at least 20 cm between the heart pacemaker and the device in order to avoid possible interferences. Turn the device off immediately if interferences are assumed.



Protection class: Observe the technical data of the respective device. In case of laser devices of class 2, the eye is protected by the blink reflex and/or turning reactions if you briefly and accidentally look into the laser beam. The devices may be used without further protective measures. Nevertheless, avoid looking directly into the laser beam of the laser scanner

Observe the additional notes in the chapter, "Proper use and environmental protection"



We declare under our sole responsibility that the product described fulfills the protection requirements of European Directive 89/336 / EEC as amended by 91/236 / EEC, 92/31 / EEC, 93/97 / EEC and 93/68 /. See the manual of the devices for the standards. Evidence is provided by compliance with the following standards:EN 55022 : 2010

- EN 55024 : 2010 + A1 : 2015
- EN 61000 – 6 – 2: 2005
- IEC 61000-3-2 : 2014
- IEC 61000-3-3 : 2013
- IEC EN 60950-1 : 2006 + A11 : 2009 + A1 : 2010

2. Introduction

Datafox data terminals have been developed to fulfill the requirements of modern personnel time recording where users have high demands concerning flexible and elegant design. Furthermore, the Datafox Embedded-Concept also covers access control. All relevant data can be recorded with modern technology and be transferred to the analysis software immediately. Billings, calculations or other analyses can be performed in a timely manner; processes can be monitored and controlled actively. This saves time and ensures the data quality and immediacy required.

Datafox data terminals are based on the Datafox Embedded-System which is equipped with modern technology for data collection and of course also data transfer. You make your entries comfortably via keyboard, touch display, RFID or barcode. The device is available with GPS, GSM, GPRS, USB etc. It fulfills all conditions for a flexible usage not only for personnel or order time recording but also for further scopes. This constitutes a real added value. The powerful tools DatafoxStudioIV and DLL facilitate quick and easy integration in any IT solutions. Due to scalability, numerous options are available. You can select according to your company's requirements and only pay what you really need.

2.1. Structure of the Documentation

The manual contains a change history as well as a general part with safety information, the introduction and information concerning system requirements and system structure.

The general part is followed by the main part of the manual. It contains the chapter Product Description Device. In this chapter, device-specific components are described as well as the device's functions.

The final part of the manual provides technical data about the device and a glossary whose purpose it is to ensure a consistent understanding between user and manufacturer.

2.2. Guarantee Restriction

All installers are responsible for the use of the device and its accessories in accordance with its intended purpose and in compliance with the applicable laws, standards and directives.

All data in this manual has been checked carefully. Nevertheless, errors cannot be excluded. Therefore, we offer no guarantee nor accept any liability for consequences that derive from errors of this manual. Of course we are grateful if you point out errors to us. We reserve the right to make modifications in respect of technical progress. Our general terms and conditions of business apply.

Note:



Due to DatafoxStudioIV, Datafox devices offer many functions and combinations of functions not all of which can be tested in the case of updates. This applies especially to setups defined by you as customer. Before updating your device, please ensure by tests that your individual setup works without any errors. If you encounter a problem, please inform us immediately. We will take care of the clarification of the problem on short notice.

2.3. Typography of the Documentation

FW	Abbreviation for firmware (software in the device)
SW	Abbreviation for software
HW	Abbreviation for hardware
GV	Abbreviation for global variable
<Name;Software Version.pdf>	File names



Note:

Useful information which helps you avoiding possible mistakes during the installation, configuration and commissioning is given here.



Caution:

Here, notes are provided which must be strictly observed. Otherwise, malfunction of the system will occur.

2.4. Important General Notes



Caution:

Use the devices only according to regulations and follow the installation, commissioning and operating instructions. Installation and commissioning may only be performed by authorized specialists.

Subject to technical alterations.



Caution:

Due to technical development, illustrations, function steps, procedures and technical data may vary slightly.

The Datafox device has been developed for the purpose of creating a flexible and easily integrated terminal for data recording serving for a great variety of applications. The device is robust and easy to use. Due to the PC setup program, the device is quickly and easily configured for its application field so that you save time.

Numerous optional features, such as bar code reader, transponder reader, digital inputs etc., enable you to use the device for:

- PZE - Personnel time recording
- AZE - Order time recording
- BDE - Operating data recording (I/O-processing)
- ZK - Access control
- FZDE - Vehicle data recording / telematics

This manual describes the creation of setups with the setup program DatafoxStudioIV without covering specific applications. Potential problems and difficulties are pointed out.

This manual describes the functionality of the KYO Fourloc and explains its characteristic features. For example, installation, operation and equipment of the device are described.

In order to define the behavior of the device, a setup must be created. For this purpose, the DatafoxStudioIV has been developed.

With some practice it will be possible to create a complete compilation for the KYO Fourloc within half an hour. If you need functions that are not available, please contact us.



Note:

If you need support for the compilation of setups, we offer you our services. Due to our extensive experience with the setup, we work very quickly and can make your setup even more efficient through useful advices, so that the input at the device can be performed quickly and securely.



Note:

Due to DatafoxStudioIV, Datafox devices offer many functions and combinations of functions not all of which can be tested in the case of updates. This applies especially to setups defined by you as customer. Before updating your device, please ensure by tests that your individual setup works without any errors. If you still encounter problems after thoroughly testing your setup, please inform us immediately. We will fix the error on short notice.

3. Intended Use and Environmental Protection

3.1. Regulations and Notices

According to the current state of the art, measures were taken to ensure that the device meets the technical and legal regulations as well as safety standards. Nevertheless, malfunctions due to interferences through other devices can still occur.

Please observe local regulations when using the device.

3.2. Power supply

Only operate the device externally with a limited power source in accordance with EN 60950-1.

If the devices run with rechargeable batteries, note the instructions in chapter "Rechargeable Battery".



Caution:

In the event of non-compliance with these instructions, the device or the battery (if any) can be damaged or destroyed!

In order to ensure maximum battery life, it is recommended to recharge the battery only after complete discharge.

See respective type label of the device KYO Fourloc.

3.3. Environmental Influences

Extreme environmental influences may damage or destroy the device and should be avoided. This includes fire, extreme sunlight, water, extreme cold and extreme heat.

See respective type label of the device.

3.4. Mounting outdoors

The KYO-Fourloc is not allowed to install outside of a building.
Only in a IP65 Case.

3.5. Temperature

The device has an approved temperature range of - 20 ° C to + 60 ° C.

A heater is not necessary for outdoor use.

Due to the inherent heat of the electronics and power supply, the temperatures in the unit are higher even at ambient temperatures below -20 ° C.

Condensation water only occurs when a cold object comes into the heat and would therefore only be an issue for mobile devices.

We recommend, if you use the devices outside, then let it running permanently. Both in terms of temperature as well as condensation, it is recommended to not switch off devices which are used outdoors.

3.6. Repair

Except for the battery replacement in mobile devices, Datafox devices are maintenance-free and must only be opened by authorized professionals. In case of defects, please contact your dealer or the Datafox service hotline.

If a definite defect is present, you can also send the device directly to Datafox.

https://www.datafox.de/reparaturen.de.html?file=files/Datafox_Devices/PDF/Support/Datafox%20Reparaturbegleitformular%20V3%2C%20D-GB_2020.09.25.pdf

3.7. Cleaning

CAUTION

Risk of explosion if batteries are replaced improperly.
Dispose used batteries according to the instructions.

3.8. Further Notices

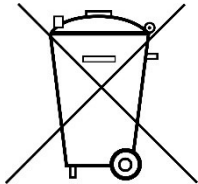
Do not expose the device to strong magnetic fields, especially during operation.
Operate the slots and connections of the device only with the appropriate intended equipment.
Ensure that the device is secured during transport. For reasons of safety, do not use the device while driving a vehicle. Also ensure that technical equipment of your vehicle is not compromised by the device.
In order to prevent SIM card misuse, have your SIM card blocked immediately in cases of loss or theft of the device.

3.9. Disposal

Observe local regulations concerning the disposal of packaging material, used batteries and scrapped electrical equipment.

This product complies with the EU Directive No. 2002/95/EC, its appendices and the Council Decision laying down the restrictions of the use of hazardous substances in electrical and electronic equipment.

The device is covered by the European Directive on Waste Electrical and Electronic Equipment which came into force on February 13, 2003 and was translated into the legislation of the Federal Republic of Germany on August 18, 2005.



Do not dispose the device in domestic waste!

As the user, it lies within your responsibility to dispose electrical and electronic equipment via the designated collection facilities. The correct disposal of electrical and electronic equipment protects human life and the environment.

For more information regarding the disposal of electrical and electronic equipment, please contact your local authorities or waste disposal companies.

4. System Requirements / Hardware

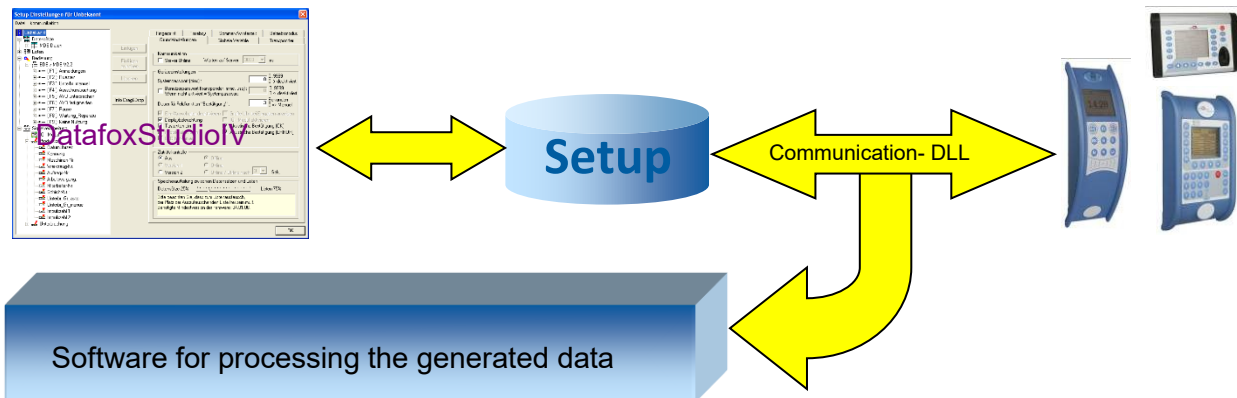
4.1. System Structure

The system consists of the Datafox device, the DatafoxStudioIV, the communication DLL and a software for processing the generated data.

Create setup

Save setup

Transfer setup to device



4.2. Installation requirements for Operating Datafox Devices

In order to operate the Datafox device, you need a 230 V power connection for the Datafox power supply. Depending on the main communication set, you need a corresponding transfer medium or connection cable.

Main communication:

- USB → one standard USB-A to USB-micro Cable (see the chapter connection USB).
- RS485 → a transmission path in accordance with the EIA-485 standard (see Connection RS485).
- 2G; 4G → a distortion-free mobile connection
- WLAN WiFi → a distortion-free channel to an access point (802.11 b/g/n) within reach (see Connection WLAN).
- at least one standard Ethernet cable, no „cross over“ (see Connection TCP)
- HTTP (internet) via LAN → TCP/IP connection with free internet access. The data are sent to a server.



Note:

With increasing demands on transfer rate and interference immunity, the demands on the transmission path increase as well with regard to quality (interference immunity).

Ideally, the cables should be provided in a flush-mounted box. Please note this please provide the height information in the assembly instructions.

Assembly instructions on our homepage:

https://www.datafox.de/d67/unternehmen/downloads/informationsmaterial/informationsmaterial-evo-serie/11500x_Datafox_EVO_4.3_4.6_7.0_Montage_und_Inbetriebnahme.pdf

https://www.datafox.de/d67/unternehmen/downloads/informationsmaterial/evo-3-5-universal/122001_Datafox_EVO_3.5_Universal_Montage_und_Inbetriebnahme.pdf

https://www.datafox.de/d67/unternehmen/downloads/zubehoer-module/zutrittsleser/12300x_Datafox_EVO_Agera_Montage_und_Inbetriebnahme.pdf

https://www.datafox.de/d67/unternehmen/downloads/informationsmaterial/evo-3-5-pure/1140x1_Datafox_EVO_2.8_3.5_5.0_Pure_Montage_und_Inbetriebnahme.pdf

https://www.datafox.de/d67/unternehmen/downloads/informationsmaterial/kyo-cenloc/124401_Datafox_KYO_Cenloc_Rack_-_TKSS_Montageanleitung.pdf

https://www.datafox.de/d67/unternehmen/downloads/informationsmaterial/kyo-cenloc/124011_Datafox_KYO_Cenloc_Wall_Bohrschablone.pdf

https://www.datafox.de/d67/unternehmen/downloads/informationsmaterial/kyo-inloc/11x402_Datafox_KYO_Inloc_HS_flach_Montageanleitung.pdf

https://www.datafox.de/d67/unternehmen/downloads/informationsmaterial/pze-master-iv/105406_Datafox_PZEMIV_Wandhalterung_Montageanleitung.pdf

4.3. General Hardware Information

4.3.1. Hardware equipment

The devices with hardware V4 are equipped with a flash memory. Depending on the device type or selected option with 4 or 16 MB.

For the data, the memory is used as a quasi-ring buffer. If the complete ring buffer is written to full without the data being retrieved, the terminal reports "Memory full", please notify the admin". No further data is stored during this time.

Data that has already been read is gradually transferred. The entire memory is always used to minimize the number of accesses per individual memory cell.

An ARM microcontroller with 32-bit technology is used.

Depending on the type of device, the device has a Goldcap capacitor for buffering the time. This ensures that the watch continues to run correctly for up to one week if the power supply is interrupted.

In other devices, such as EVO 4.3 or PZE-Master V4, a buffer battery is installed in addition to the capacitor. With this, the watch retains its value for approx. 4 years.

The exact equipment can be found in the last chapter Technical Data.

4.3.2. Behavior in case of power failure

The device boots automatically when the power supply is switched on again.

All data that was not sent or retrieved by the application software before the power failure is stored on the device.

These are not lost. After booting, this data is available again.

4.3.3. UPS

A corresponding UPS for the V4 hardware is in preparation.

We currently recommend equipping the devices with a POE module if a "UPS" is to be used. Then connect the devices via a POE switch and supply the switch via a standard UPS.

4.4. Compatibility

The compatibility must be observed urgently between:

- Datafox devices and the device firmware
- Device firmware and device setup
- Device firmware and communication DLL
- Communication DLL and DatafoxStudioIV
- DatafoxStudioIV and device setup

4.4.1. Firmware File Archive (*.dfz)

Description

The Firmware archive combines device specific firmware files into an archive container. This archive uses the file extension DFZ (abbreviation for Datafox Zip). When uploading firmware to a device through DatafoxStudioIV or the DFCom library, simply use this archive.



Note:

The firmware archive does not only contain software for the current device generation (HardwareIV), it contains software for previous hardware versions as well. You can update any Datafox device using this archive and upload the current version of the device firmware in this way..

Function of the Archive

The transfer routine of the device file selects the right file from the firmware 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.

4.4.2. Datafox Devices and Device Firmware

Each Datafox device has an electronic flat module. The module has specific hardware equipment concerning the options (e.g. mobile radio, WLAN, fingerprint, ...). Due to technical conditions, different options are mutually exclusive. Currently there are conditions where not all hardware options can be supported in one firmware file due to limited program memory. This means that each device with specific hardware options needs a proper firmware to support the hardware options by the software.



Caution:

In general, the newest version of DatafoxStudioIV should be used, since this version is capable to support the current device hardware version. Should you opt for using an older version of DatafoxStudioIV, please keep the following minimal version requirements in mind:

- DatafoxStudioIV Version 04.03.00.x or newer is offering support for Hardware Generation IV and III
- DatafoxStudioIV Version 04.02.00.x or newer is offering support for Hardware Generation III

4.4.3. Device Firmware and Device Setup

The firmware (operating system) of the device and the device setup (*.aes data file = application program) form a unit. By the device setup, the runtime behavior of the device (the firmware) is determined. This means the response of the device to input events by the user or the environment (e.g. digital inputs). In principle, only those functions of the device are executed that are supported by the firmware and defined via the setup. Prior to the productive commencement, you should therefore test each setup with the corresponding device or on a device with the same hardware options and firmware.

4.4.4. Device Firmware and Communication DLL

A firmware supports certain functions, dependent on the hardware options. The communication DLL is the interface between the firmware and the DatafoxStudioIV or your processing software. Therefore, the firmware must always have the same or a lower version number as the communication DLL.



Note:

If your application uses a newer version of the communication DLL than the firmware does, you can only use functions that are supported by the firmware. Otherwise, you will receive an error message (e.g. function not supported) which has to be analyzed.

4.4.5. Communications DLL and DatafoxStudioIV



Note:

The DatafoxStudioIV and the communication DLL are developed and released as a bundle. Therefore, they have to be used as a bundle. A newer version of DatafoxStudioIV does not work with an older DLL.

4.4.6. DatafoxStudioIV and Device Setup

With the DatafoxStudioIV, you create a device setup (application program) for the Datafox device. That means that in the setup only those functions were defined which were available in the DatafoxStudioIV version at the time of the setup creation. The DatafoxStudioIV you use for opening a device setup may thus only be newer but never older than the DatafoxStudioIV version you used to create the device setup.



Note:

The updates are always available for download on our homepage www.datafox.de.



Caution:

When new devices are delivered, the latest firmware is loaded on the devices. If you wish to work with an older firmware version, please perform a downgrade. Please observe the compatibility notes in the release notes of the respective firmware version.

The data file <Device name>, Software version <version number>.pdf shows which functions are supported by which software release.

You will find the file on the product CD. Please also follow the instructions given in the chapters of the manual.

4.4.7. Update / Downgrade

A firmware update or downgrade is a very sensitive process. Possibly, a reset of the main communication to RS232 may occur. In any case, consider the information regarding the compatibility in the software version list.

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 observed.

For example: when changing from Version 04.00.xx to version 04.01.xx, at least version 04.00.23.769 or higher must be present in order to run the update to version 04.01.xx successfully.

Firmware Downgrade

A firmware downgrade is not recommended.

We are constantly working towards improving the software/firmware; all functionalities are still included in new versions. New software always offers better functionalities and possible bugs are fixed.



Caution:

When performing a firmware downgrade the firmware has to be transmitted to the device twice. This has technical reasons. Errors shown on the display of the device after the first transfer can be ignored.

5. Device

**Note:**

It has to be taken care of a suitable protection from direct sunlight because the synthetic materials are not 100% UV resistant. Fading simply is an optical defect which does not restrict the function of the device.

**Caution:**

Please 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.

5.1. Commissioning

On delivery, the device is fully functional and configured with a demo setup so that you can test the input immediately. After establishing the power supply the device will switch on automatically. The KYO Fourloc automatically starts booting, recognition of the hardware options and loading the setup. After having finished booting, the device switches to operation. Now itKYO Fourloc is ready for use.

**Note:**

On delivery, the main communication is set to USB.

**Caution:**

If external modules (e.g. access control, signal processing via the digital inputs) with an external power supply are used, ensure to comply with all limits (max. voltage and current) before commissioning the system.

5.2. Guideline for Commissioning

5.2.1. Set-up of the device

This section provides a short guideline for commissioning und links to the corresponding chapters in the manual.

- ▶ Connecting device to current supply
- ▶ Setting interface for communication
- ▶ Loading setup of the device See manual „[DatafoxStudioIV](#)“



Attention:

The main communication interface must be set using the DatafoxStudioIV program.

5.2.2. Installation of the device

- ▶ Installing the device at the intended location
- ▶ Establishing connections for:
 - Power:
 - Communication:
 - USB
 - TCP/IP
 - TCP/IP wLAN /Wi-Fi
 - GPRS
 - RS485
 - Digital input
 - Digital output
 - Analog inputs
 - [Access-control](#)
- ▶ Finishing installation of the device
- ▶ Setting for main communication

5.2.3. Troubleshooting during Commissioning

- ▶ Please see the FAQ on our website: <http://www.datafox.de/faq-de.html>.
- ▶ Tips:
 - Connection to the device cannot be set up via TCP/IP
 - Check IP in the device and the application (studio)
 - Ping on IP
 - Setting "Active Connection" in the Active.ini → set to 0
 - Setting "HTTP" in the http/GPRS.ini → set to 0

5.3. Communication of Hardware V4 Devices



Caution:

The type of communication depends on the device.
All possible communications are listed in the device.



Note:

Datafox-devices are able to communicate encrypted.
Read more in the manual for the „DatafoxStudioIV“.

The switching of the communication can be done via :

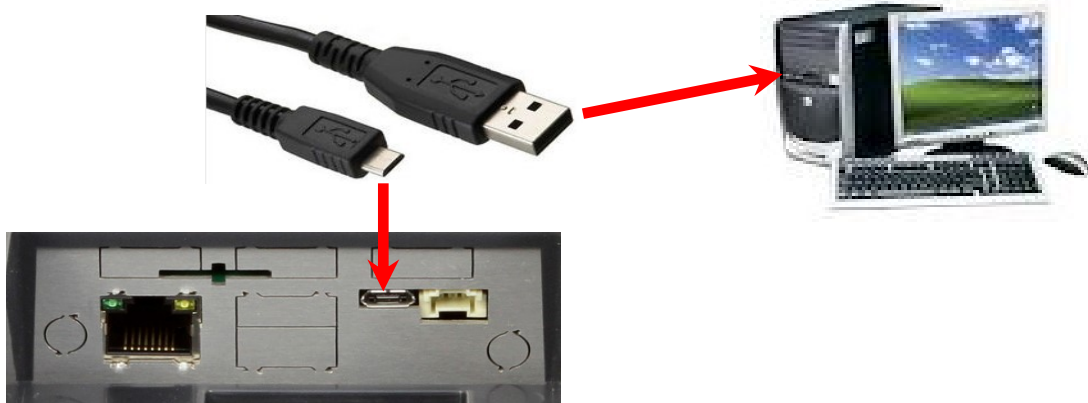
1. the system menu bios on the device
2. with firmware version 04.02.04 and up with the function „Switch communication“.
3. from the Firmware version 04.02.04 upwards with the field function „switch communication“.
Read more in the manual for the „DatafoxStudioIV“

Possible communication types are:

1. USB (on PC)
2. USB Host, Save data on a USB-stick
GPRS connection with mobile cell network.

5.3.1. Communication via USB

Every EVO-Line Device is equipped with an USB interface.
The USB-C Port can be connected directly to a PC.



Caution:

The Terminal works with a USB-B Interface. This means that the device works in slave mode only. So it is not possible for the device to control any other devices via USB.

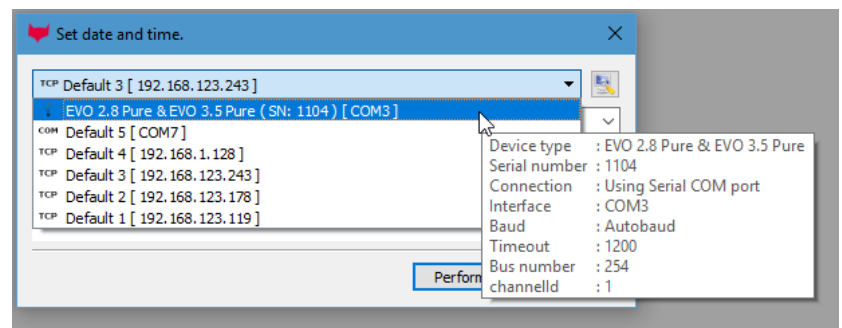
5.3.1.1. Automatic detected connected USB to PC

If the terminal is connected to a PC it will recognize the connection and will switch the communication to USB.

DatafoxStudioIV will recognize the device and a notification will pop up.



The studio will generate an entry for the device.



following icon is displayed:



It is not necessary to switch the main communication to USB manually.

It's especially useful for boxed devices.

This will save much time in the parameterizing process.



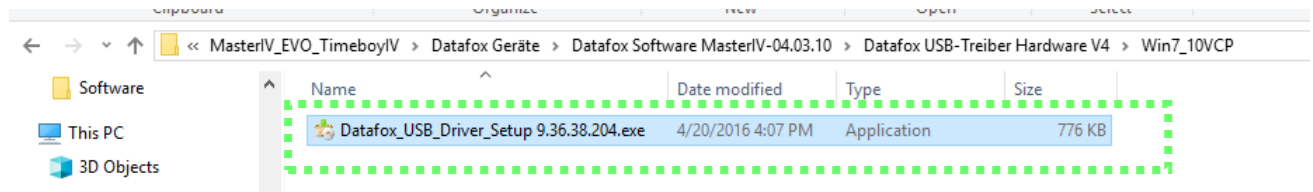
Note:

If the device is connected to a PC no other connections (for example Wi-Fi) will happen. If the USB-cable is disconnected, it will automatically switch to the configured main communication.

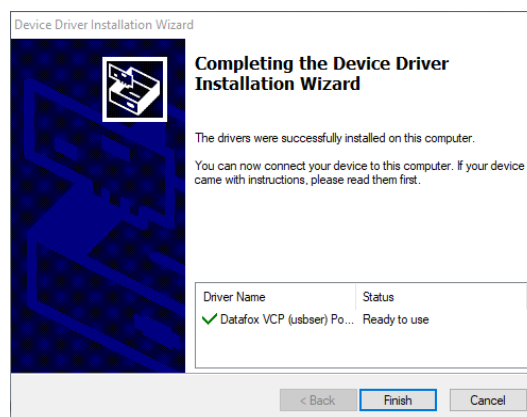
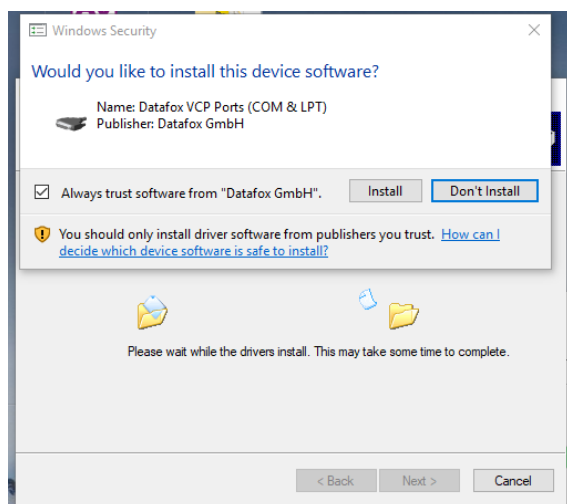
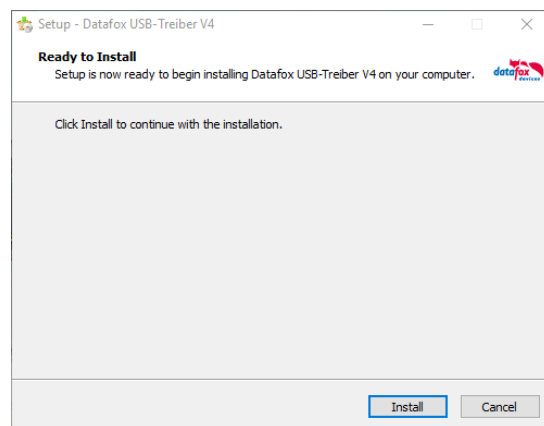
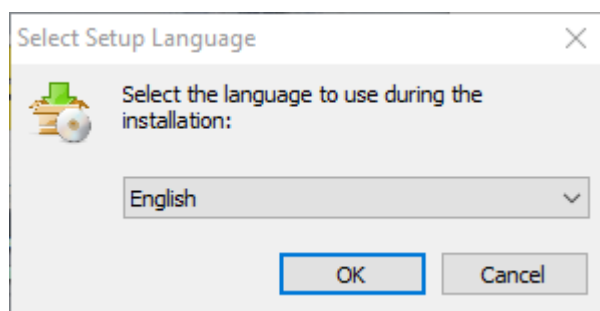
5.3.1.2. Installing USB driver for Hardware V4 Devices

Installation for Windows 10 and 11

The USB-Driver is a small installer which will do the necessary configuration. Just launch the .exe file.



Follow the instructions on the screen:

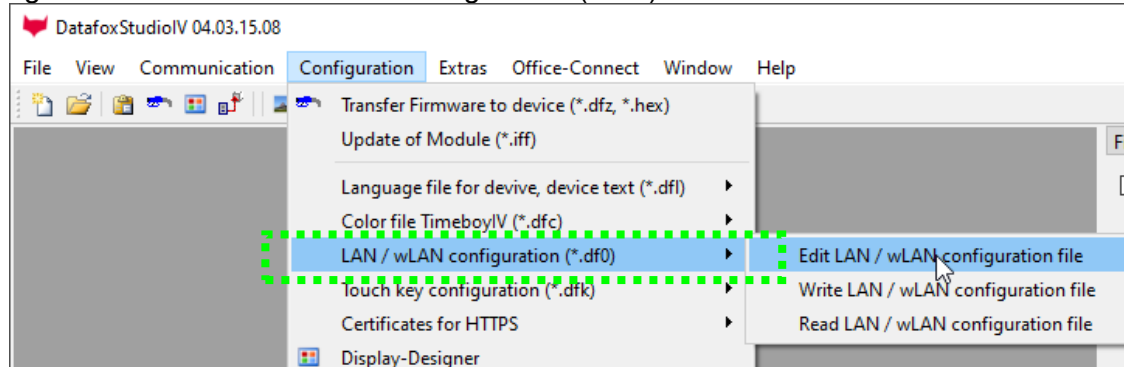


Caution:
 Only use the driver which are delivered with the device!

Note:
 If you have DatafoxStudioIV installed, the USB-driver will already be installed on your PC.

5.3.2. Communication via TCP / IP

The setting of the LAN / WLAN parameters is done via DatafoxStudioIV under the menu item "Configuration" → "LAN / WLAN – Configuration (*.df0)".

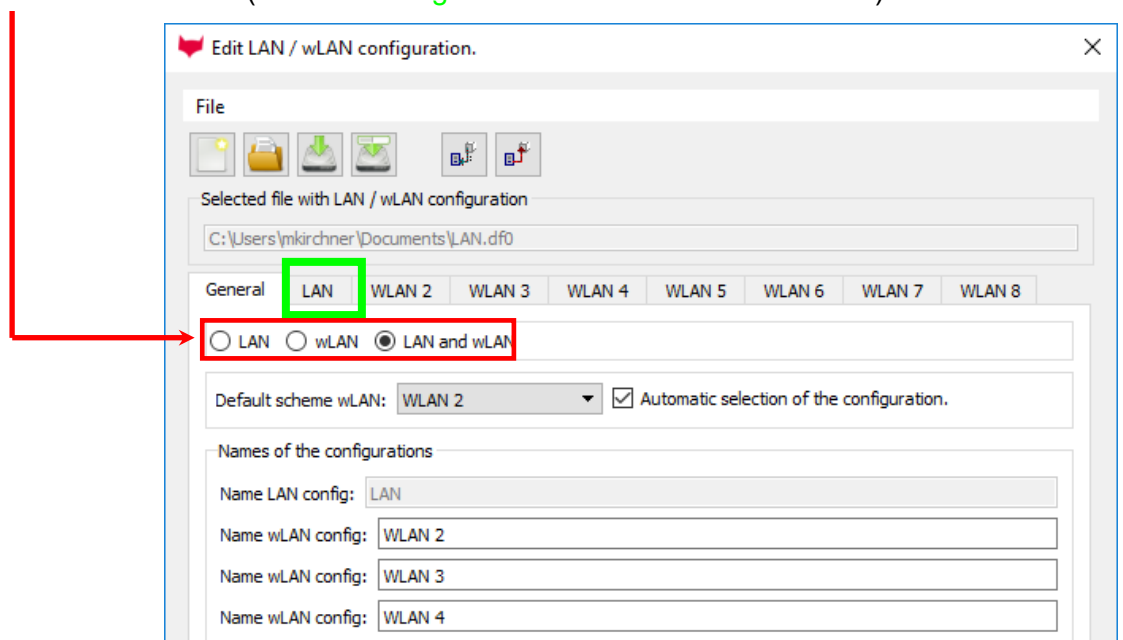


The LAN / WLAN configurations are saved in a file with the filename extension "*.df0". Here you have the possibility to edit the file, load it into the Datafox device (upload) or read it from the device (download).

When reading the WLAN setting from the device, the currently specified file is overwritten.

In the General tab, first of all, you can set the main communication with which the device is equipped.

- Device with LAN (The first configuration is for LAN connection)
- Device with WLAN
- Device with LAN and WLAN (The first configuration is for the LAN connection)

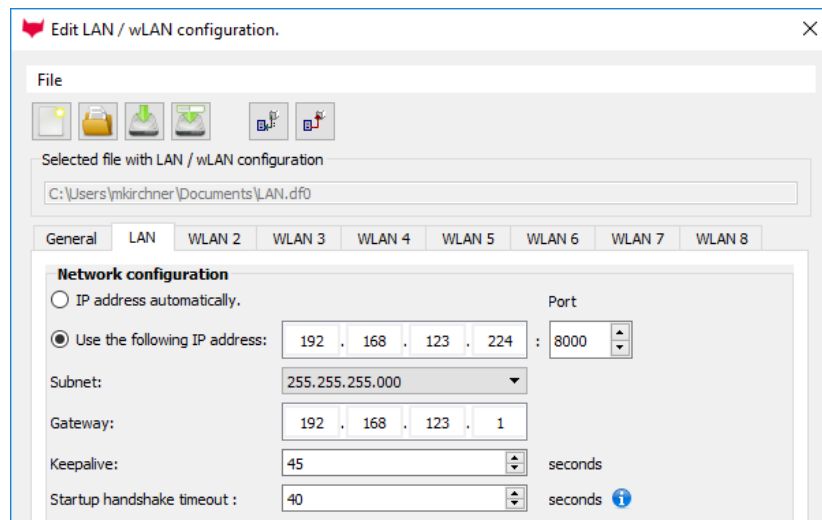


Caution: For TimboylV only this setting (only wLAN) can be used.

5.3.2.1. Communication TCP / IP via network-cable

You can make the IP settings on the "LAN" tab.

Please enter the desired IP address, subnet and if necessary a gateway.



For devices with display, the IP address can also be entered directly on the device. Press ESC and ENTER simultaneously to enter the Bios menu of the device.

More information can be found in the chapter „bios menu“.

5.3.3. Communication TCP / IP via wLAN / Wifi

General information about the WLAN modules used.

There are 2 different WLAN modules that have been integrated into the Datafox devices.

- 1.) Redpine – installed in the units since 2013.
- 2.) Texas Instruments TI-CC3135 - installed in the devices since 2021.03.

Basically, both modules can be set via the DatafoxStudioIV or on the device itself. The only difference between the modules is that different standards are supported. You can see what each module supports in detail on the following pages.

You check with the DatafoxStudioIV via Configuration -> Device configuration (Bios):

Standardmodul	014 RS485 + 12V Supply	1	M1	
Standardmodul	012 Digital In-/Output	2	M2	DI 1, DO 1
Standardmodul	WLAN TI CC3135 ML01	4		
Standardmodul	037 Single Serial Port	6		
Transponderleser	TSR32 Reader 125kHz	1		
Standardmodul	014 RS485 + 12V Supply	7	M7	

oder:

 Standardmodul 001 WLAN Redpine RS9110 6 - Vers. 4.5.5, Mac: 88-DA-1A-7F-E6-65, Ip: 192.

You have a delivery note and look at the article number

- 1.) Redpine: Art.Nr.: xxx112 (generation 1)
- 2.) Texas Instruments CC3135: Art.Nr.: xxx112 A (generation 2)

You are checking the Bios menu of the unit:

Under: System Menu-> System Menu
 Bios-> Communication
 Here you have to set the unit to "WLAN"
 as the main communication.
 Under the settings WLAN parameters
 you have an info menu „Modul Infor-
 mationen“.



5.3.3.1. M111_WLAN ESP32-c3 ML01 (wLAN-Modul DF-WL03)

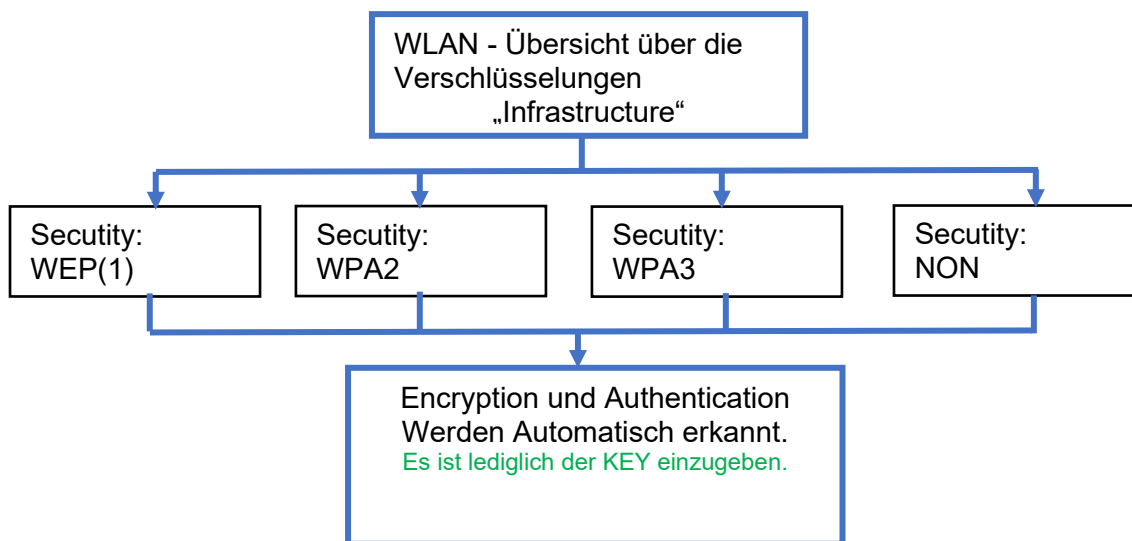
This overview shows you which **WLAN** methods are supported.

The WLAN 3 module automatically detects the encryption of the AP. Therefore, only the Security parameter needs to be set. The other parameters (Encryption and Authentication) are detected automatically.

Routers that operate WPA3/WPA2 in mixed mode can already be used now.

Router die WPA3/WPA2 im Mixed Modus betreiben können bereits jetzt genutzt werden.

Supportet is here only the 2.4Ghz.



Achtung:

Wir können nicht jeden auf dem Markt befindlichen Access-Point Testen.
Daher ist es uns nicht möglich, einen Verbindungsaufbau zu jedem AP zu garantieren.

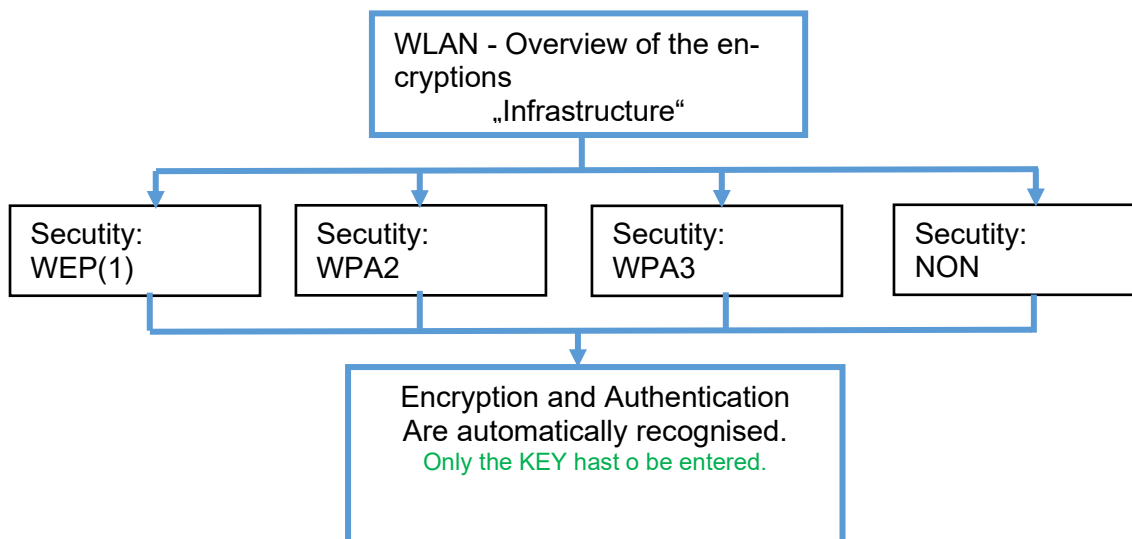
5.3.3.2. Texas Instruments TI-CC3135 (Generation 2)

This overview shows you which **WLAN** methods are supported.

The TI-CC3135 module automatically detects the encryption of the AP. Therefore, only the Security parameter needs to be set. The other parameters (Encryption and Authentication) are detected automatically.

Routers that operate WPA3/WPA2 in mixed mode can already be used now.

If the networks in the 5Ghz and 2.4Ghz bands have the same name, the network with the better reception quality is selected. This is usually the network in the 2.4Ghz band.



Attention:

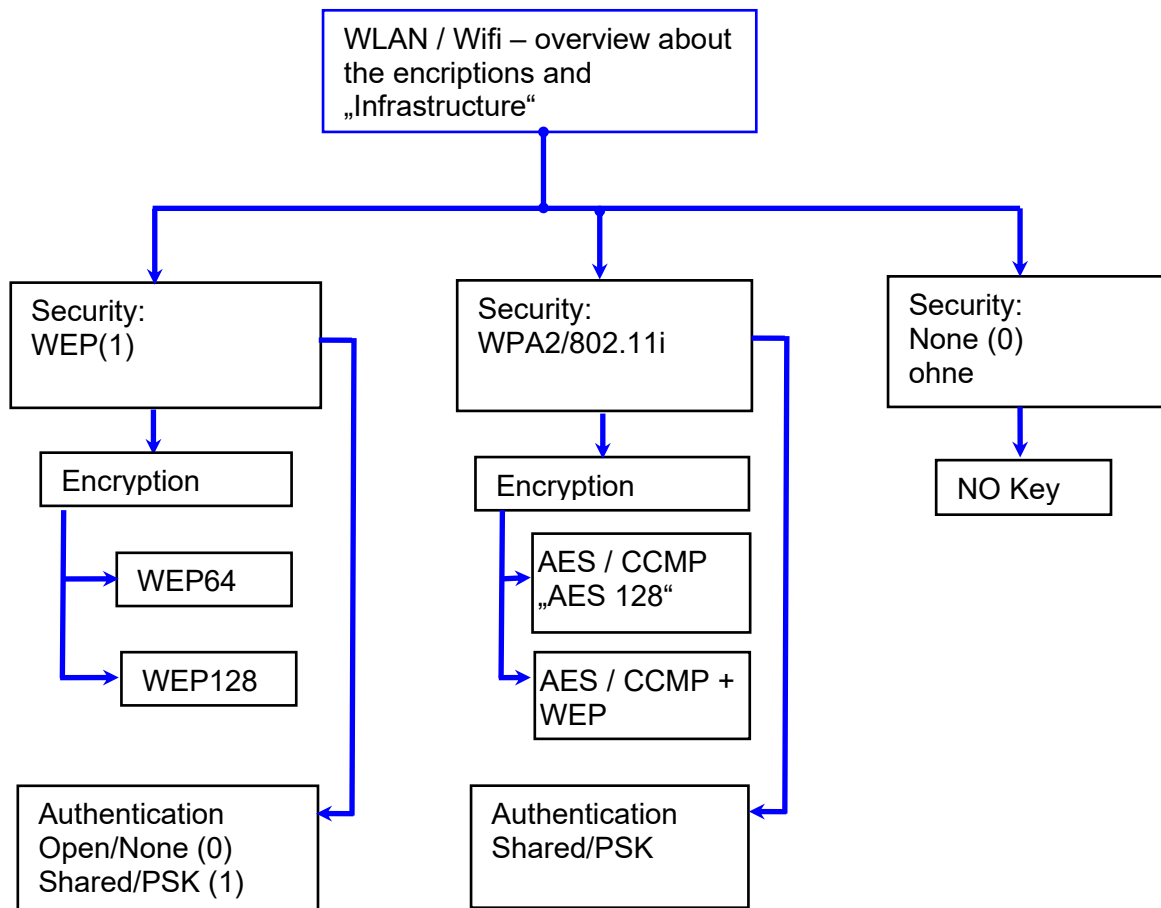
We cannot test every Access point on the market.
Therefore, it is not possible for us to guarantee a connection to every AP..

Support for WPA3 and WPA2 Enterprise is planned.

5.3.3.3. Redpine (Generation 1)

This overview shows you which WLAN methods are supported.

- **Not supported** is WPA (Predecessor of WPA2).
- **Not supported** is multiple-input multiple-output (MIMO)
- **Not supported** 5 GHz connections and no mixed operation 2.4 GHz / 5 GHz
- **Not supported** Authentication via WPA2 Enterprise according to IEEE 802.1x



Attention:

We cannot test every available Access-Point on the market. Therefore, it is not possible for us to guarantee a connection to any AP.



Attention:

[multiple-input multiple-output](https://en.wikipedia.org/wiki/multiple-input_multiple-output) (MIMO) are not supportet. If you switch the access-Point AP from b/g/n to b/g, use the access-Point only SISO. https://en.wikipedia.org/wiki/Single-input_single-output_system

When setting the encryption AES or WEP, only one type is used at a time.

The setting AES+WEP means for some access points that AES encryption is performed first and then additionally encrypted with WEP.

In this case, only set AES.

Select the configuration or location for which you want to set the WLAN parameters.

Enter the IP address for the device here. This must be the same for every location.

All the settings required for an access point can be made here.

If a key is stored, this will be displayed.

If you check this box, the battery life will be significantly increased if the device is operated with a rechargeable battery. **Important for TimeboyIV!**

A scan (search) for access points is only carried out after a disconnection after this set time. Please note the following Attention Box!

Attention:



A search for a new access point requires a lot of energy and drains the battery. Avoid a continuous search for an access point when the device is operating at the limit by generously selecting the pause between scans for new access points (80-120s). At most access points there is the possibility to set the "Beacon Interval". The higher this is set, the less power the TimeboyIV needs. Recommendation: Beacon interval >300ms.

The entire file with all settings is transferred to the device. If the device has a display, the location can be selected in the Bios menu -> Communication -> WLAN. Each location has its own configuration for the WLAN connection. The user therefore has no insight into the dial-in parameters at the various locations.



Hint:

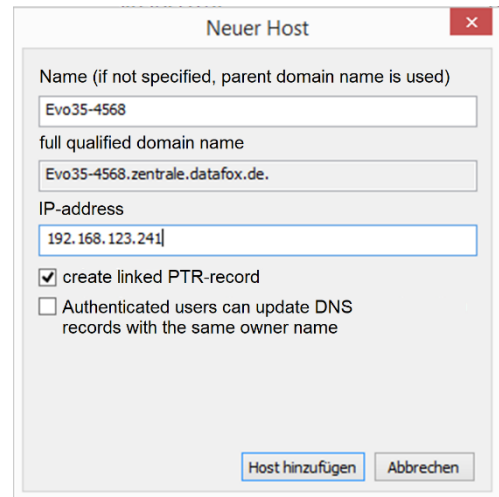
With automatic selection of the configuration / location, the first attempt is always made to establish a connection with the default schema.

5.3.3.4. Connection of the Terminals via TCP/IP DNS / DHCP

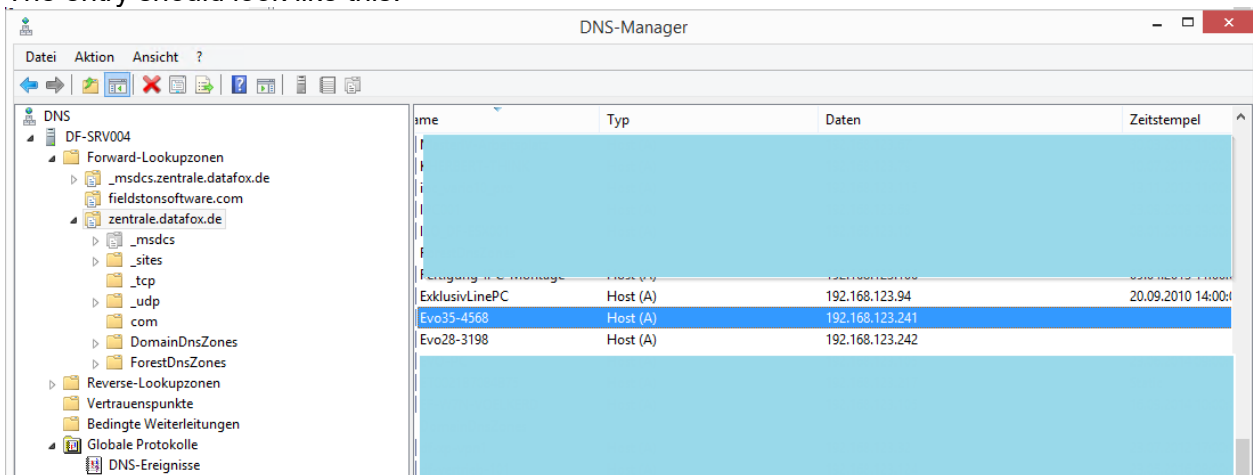
To connect a Datafox EVO-Device with the Hostname it is necessary to set something in the DNS-Server. (In this example Windows-Server 2012)

Create a new Host (A)-value:

Abbreviation	Description
Name	Name of the device Contains the device designation and the serialnumber „deviceXX-serialnumber“ Example: „Evo28-1652“ „EVO43-8552“
full qualified domain name	This is the host name to be entered later.
IP-address	Here you must enter the IP of the device.
Create linked PTR-record	You must create a linked PTR-record. Just put this hook.



The entry should look like this:



Name	Typ	Daten	Zeitstempel
ExklusivLinePC	Host (A)	192.168.123.94	20.09.2010 14:00:00
Evo35-4568	Host (A)	192.168.123.241	
Evo28-3198	Host (A)	192.168.123.242	

Settings in the DatafoxStudioIV:

Host name

Before entering, this checkbox must be set.

DHCP- entry for Datafox devices

If a device is set to DHCP, the IP address and the entry in the DHCP server can look like this.

192.168.123.109	Evo43-36100.zentrale.datafox.de	10.07.2017 23:01:31	DHCP	e4f7a100000c	Vollzugriff
192.168.123.223	Evo43-1292.Zentrale.datafox.de	Reservierung (inaktiv)	Keine	e4f7a100072f	Testgeraet Le... Vollzugriff
192.168.123.226	Support_ZK-Box V4	Reservierung (inaktiv)	Keine	e4f7a100073f	Vollzugriff
192.168.123.112	PZE-17358.zentrale.datafox.de	10.07.2017 23:51:21	DHCP	e4f7a1001964	Vollzugriff
192.168.123.125	Evo28-3705.zentrale.datafox.de	10.07.2017 14:05:02	DHCP	e4f7a100370d	Vollzugriff
192.168.123.72	Evo43-5002.zentrale.datafox.de	10.07.2017 22:58:05	DHCP	e4f7a1005070	Vollzugriff

The entry contains the following:

device	serial number	domain	DHCP- entry
EVO 2.5	10245	.zentrale.de	Evo25-10245.zentrale.de
EVO 3.5	10246	.zentrale.de	Evo35-10246.zentrale.de
AE-Master	10247	.zentrale.de	AE-10247.zentrale.de
PZE-Master	10248	.zentrale.de	PZE-10248.zentrale.de
EVO 4.3	10249	.zentrale.de	Evo43-10249.zentrale.de

5.4. Operation with Box-Devices V4

5.4.1. Bios Menu of Box Devices V4



Caution:

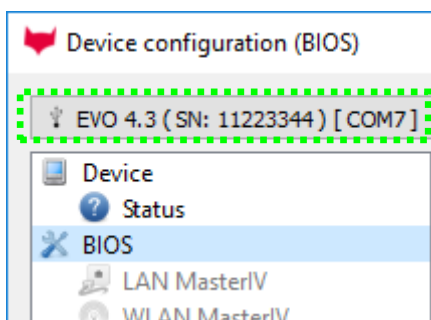
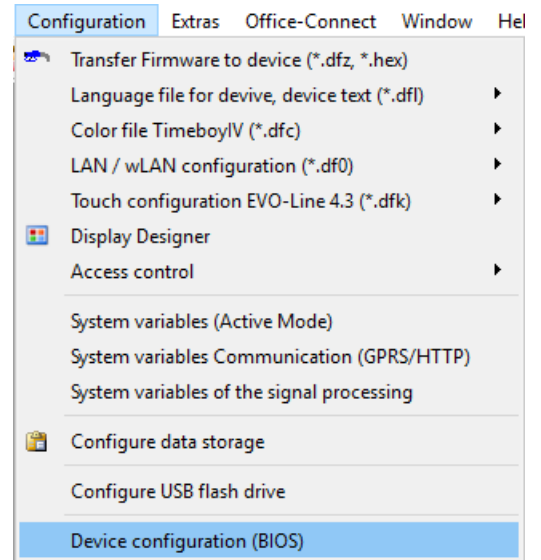
This device has no display. All settings you must do via the programm „DatafoxStudioIV“.

Open the Programm „DatafoxStudioIV and connect the device via USB.

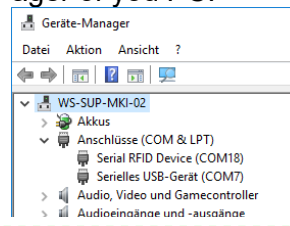
<https://www.datafox.de/downloads-software-masteriv-hardwareversion-v4.de.html>

Click on **Configuration**

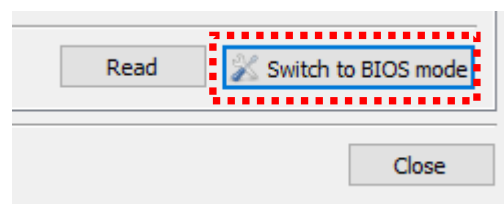
Click on
„Device configuration (Bios)“



Use the corectly com port.
You see the Datafox Virtual COM Port in the device manager of you PC:



Click on,
„Switch to BIOS mode“



Device

- Status
- BIOS**
- LAN MasterIV
- WLAN MasterIV

Description	Value	[P]	[M]	Additional info
Device name	EVO 3.5			
Serial number	5385			
Firmware version	04.03.10.06.EVO35			
Bootloader version	04.03.03.07			
Password key	0000000000000000			
DataOnCard	Funktion Datenübertragung			
Mainboard	IO-Box Mainboard	0	-	Vers. 1.4c
Default module	029 POE Supply	14		
Default module	014 RS485 + 12V Supply	1	M1	
Default module	012 Digital In-/Output	2	M2	DI 1, DO 1
Default module	012 Digital In-/Output	3	M3	DI 2, DO 2
Default module	037 Single Serial Port	6		
RFID reader	TWN3 Multi NFC Reader	1		
Communication	011 Ethernet Port	8	-	Vers. 2.0.3, Mac: E4-F7-A1-00-2A-6A, Ip: 192.168.123.241:8000
Default module	057 Graphic Adapter	11		
Display	Color TFT 3.5" 320x480	1		

[Read from text file](#)

Information [save as text](#) or [Send support mail](#).

Command message:

✓ Execution was completed successfully.

Click on
"Switch to BIOS mode"

Device

- Status
- BIOS**
- LAN MasterIV
- WLAN MasterIV

Interface

Interface:

Baud-rate:

Device ID:

Additional commands in the BIOS

Volume of the buzzer: (Range 1 - 100)

Command message:

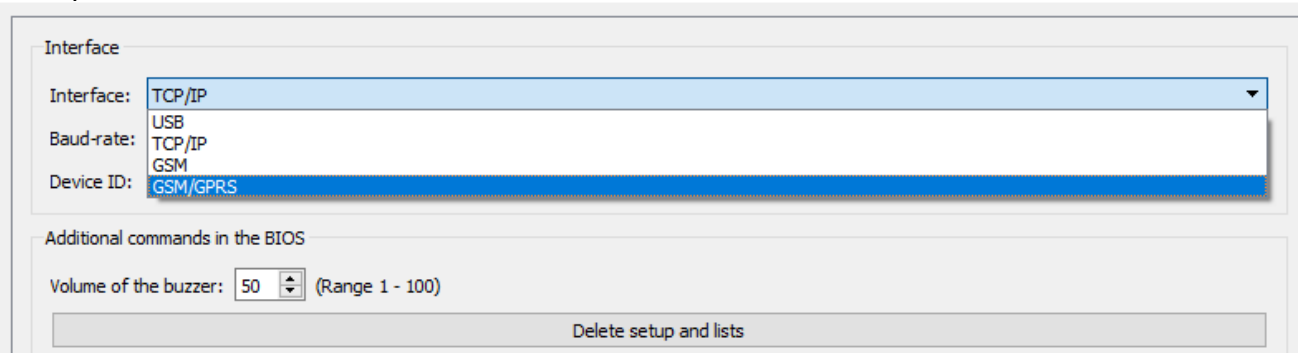
i Please click on the button <Read> to determine the current settings.

Switch communication:

In this menu, the currently set interface can now be read out.

A drop-down menu will show you all the options for the adjustable interface available on the connected device.

Example:



Interface

Interface: TCP/IP

Baud-rate: TCP/IP

Device ID: GSM/GPRS

Additional commands in the BIOS

Volume of the buzzer: 50 (Range 1 - 100)

Delete setup and lists

The volume of the buzzer can also set here.



Caution:

All new settings first accepted after a device reboot.



Note:

Further information about GPRS, TCP/IP setting you find in the Manual "DatafoxStudioIV".

5.4.2. Anzeige der Status LEDs beim Fourloc



- **ON** Spannung liegt an (rechts)

- Kommunikation aktiv (links)

- Service / Fehler (rechts)

- Datenspeicher aktiv (links)

aus = keine Daten
an = Daten im Speicher
blinken = Datenspeicher voll



USB - C Anschluss

Status-Meldung der Box	LED On grün	LED Online grün	LED Service rot	LED Data gelb
Start Setup	ein			
Power off	aus	aus	aus	aus
Booten + alle LEDs Kurz ein	10 Hz	aus	aus	aus
No Setup			1 Hz	
Kommunikation aktiv		50 ms blinkend		
Daten im Gerät				ein
Speicher voll				Blinken Ältesten Daten werden überschrieben.

5.5. Mounting of the Fourloc

5.5.1. Mounting on a hat-rail

The device is only designed for mounting on a top-hat rail.

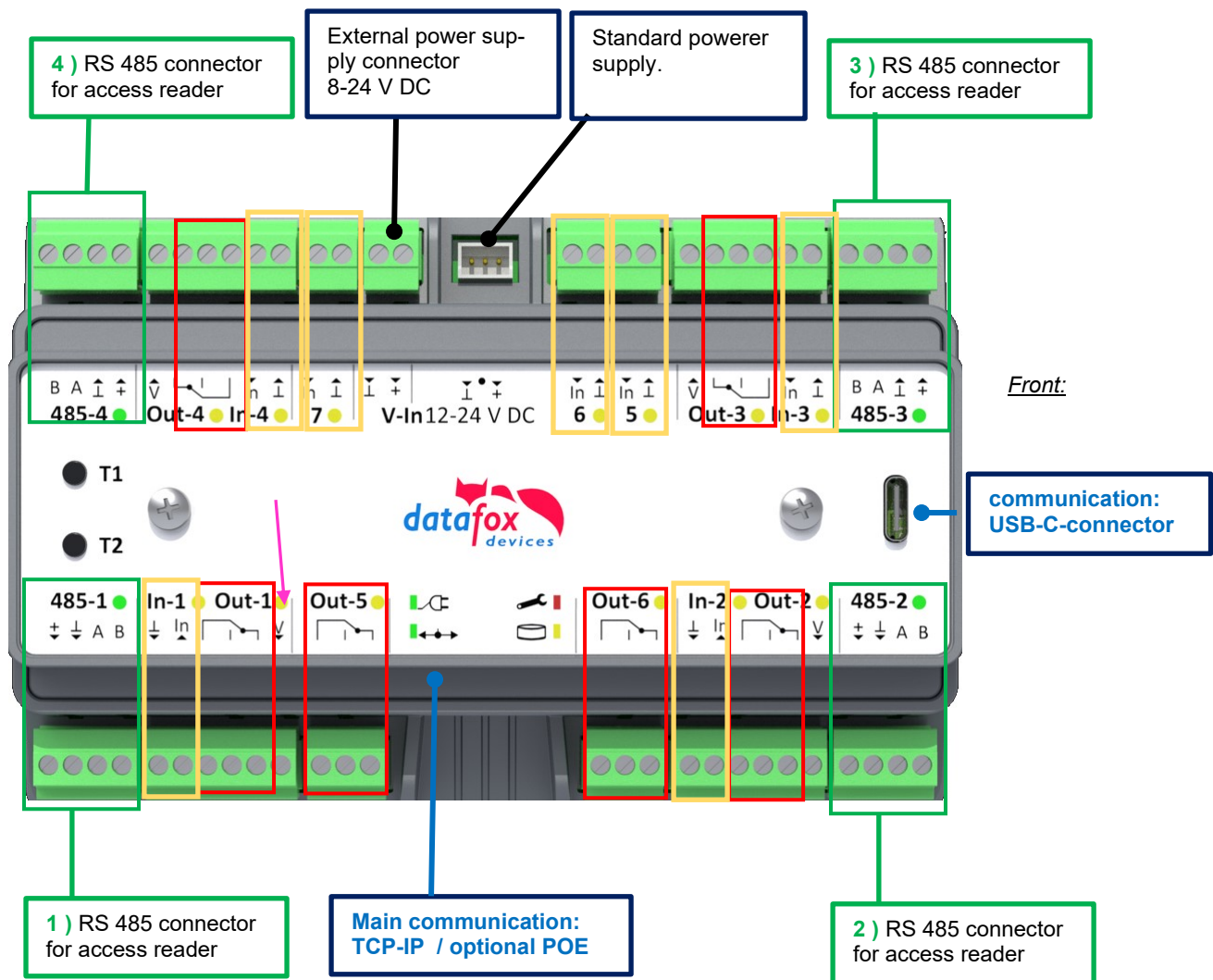


Example:
The device is installed in an electrical distribution box.



5.6. Connecting of the KYO Fourloc

5.6.1. Connectors of the KYO Fourloc



**digital output 1 bis 6
with potential-free changeover contact**

**Digital input 1 bis 7
Contact open = LOW-Signal
Contact with cable bridged = HI-Signal**

V = power output.
Outputs the voltage from the power supply 1:1.
Can be used for the door opener.

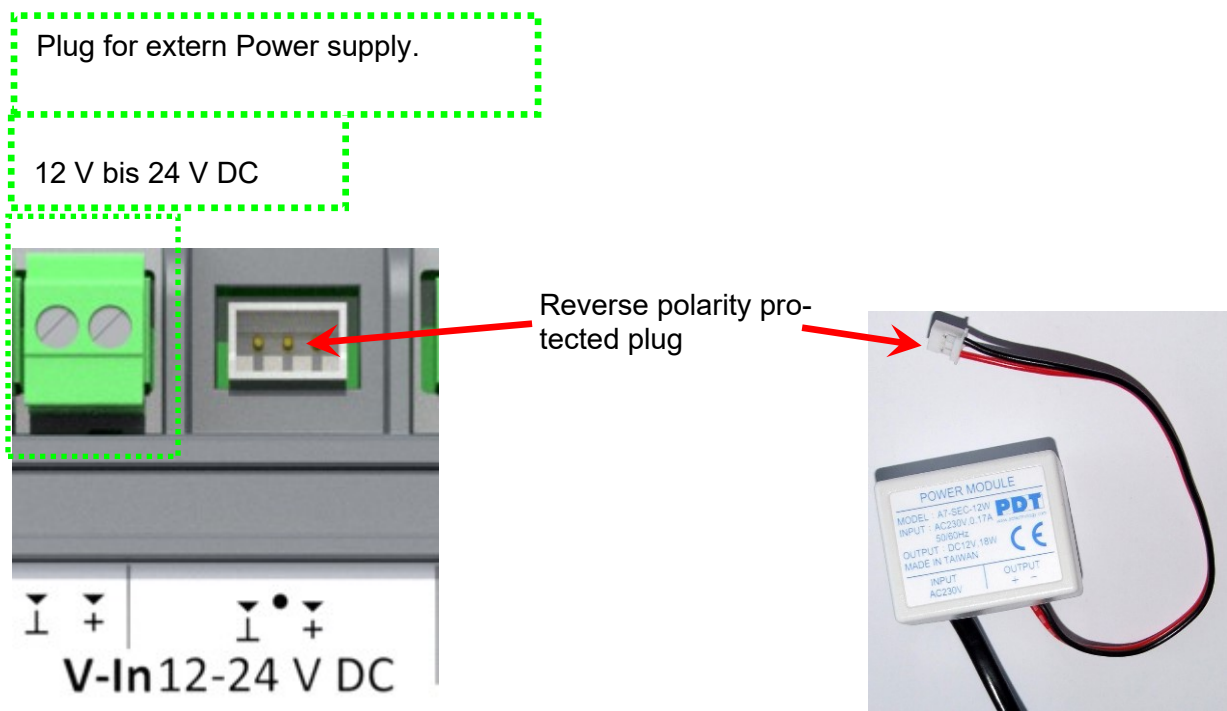
Note:
The device has no optional extensions.
Only the standards can be used as described!

5.6.2. Power supply for the KYO Fourloc

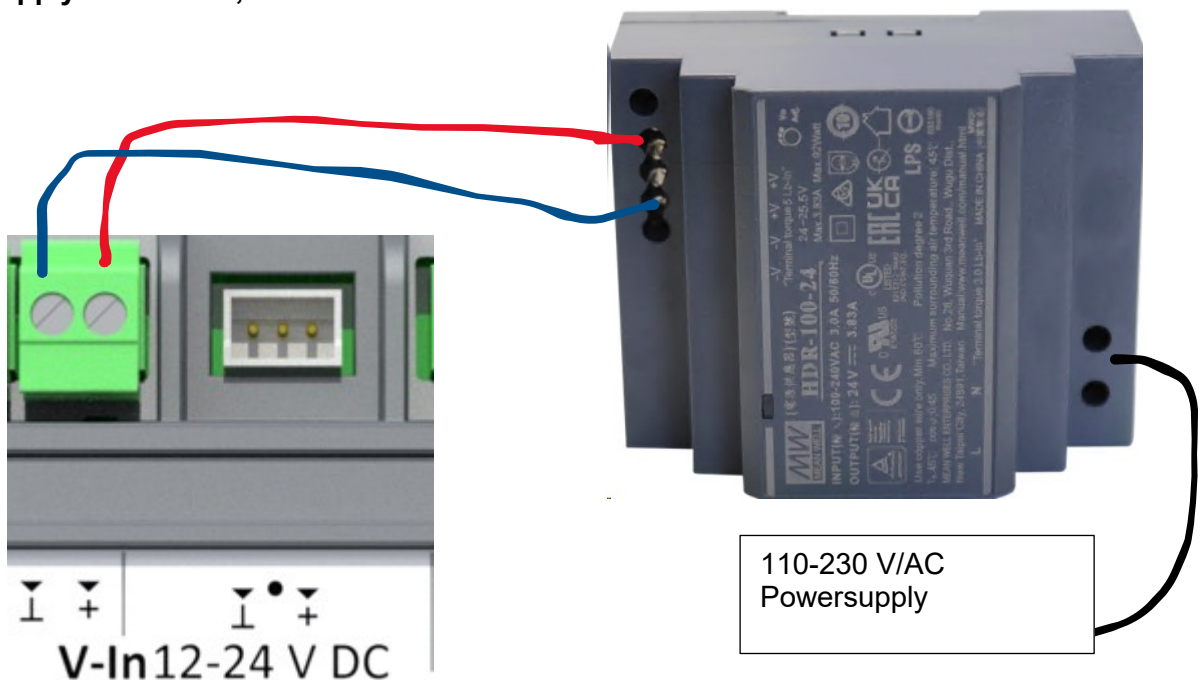
The supply voltage is provided by a 12V/24V DC power supply.
The terminal itself can be supplied with a supply voltage of 24 V DC.

Danger! The supply voltage is passed on directly to the Access modules.

The standard power supply 12V /DC:



Power supply for DIN rail; 15V /DC:



5.6.3. Power via POE

An option to order is POE.

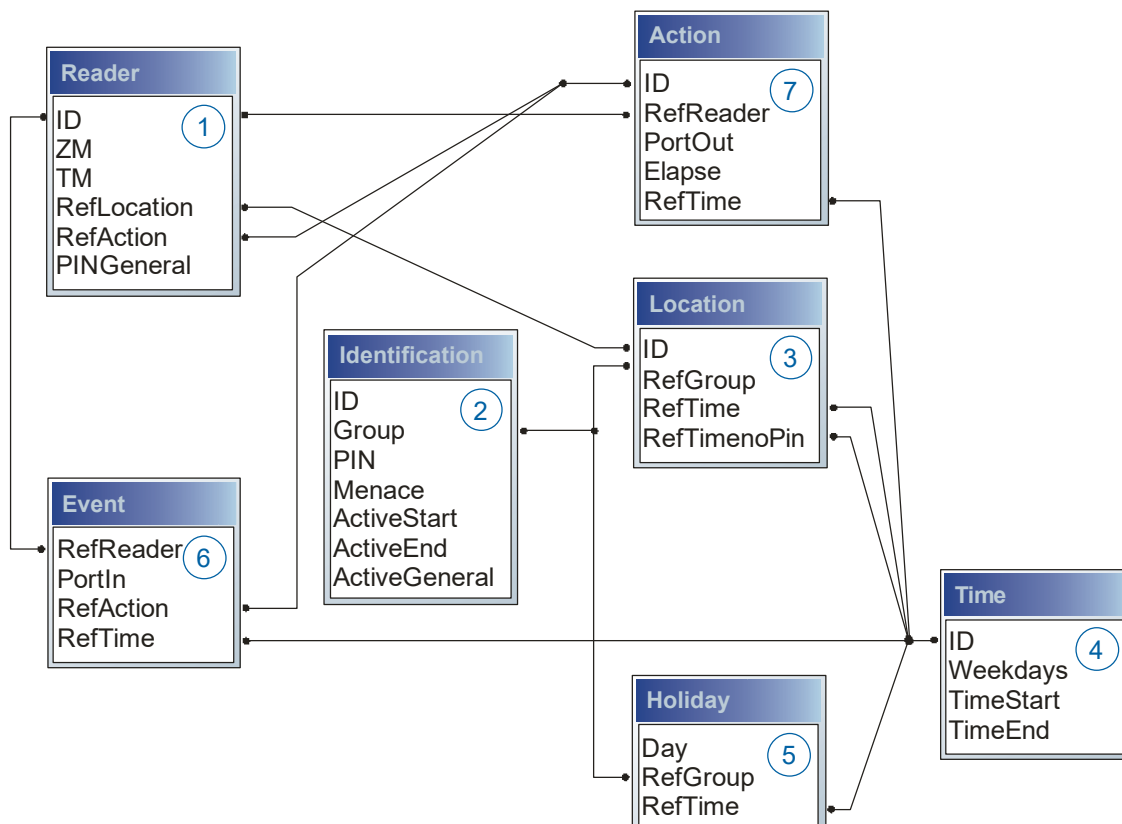
PoE-Standard		Leistung pro Port	nutzbare Leistung
PoE+	IEEE 802.3at	25,4 Watt	21,90 Watt

Erfolgt die Spannungsversorgung über POE, kann bei angeschlossener Zutrittskontrolle auch ein Externer Leser über den Anschluss der ZK mit versorgt werden.
Es können somit 4 Leser angeschlossen an je ein ZK-Modul über POE mit Spannung versorgt werden.

5.7. Connection and wiring of the access control

5.7.1. Configuration and structure of the Access control

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 employees, periods of time (activation, blocking times, holidays,...). The tables are connected as follows:



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

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.

The table Reader.txt might look like this:

ID	ZM	TM	RefLocation	RefAction	PinGeneral
1	1	320	0	1	0
2	1	000	1	2	0
3	1	010	2	3	0

Holiday Control

It is now possible for ZK-II to consider holidays at switching the relay. In order to achieve compatibility with older versions, the function consider Holidays for the Time Control of Relays has to be activated at the setup page Access Control 2. In the column Group, you specify the **Action ID** of the switched relay output instead of a Group ID. Thus, it is not necessary to alter the table structure of the holiday list. The column RefTime provides the time model applicable that day. A minus sign must be inserted in front of the Action ID in order that the MasterIV terminal can differentiate between Action ID and Group ID. As a result, these Action IDs must be three-digit numbers.

Example:

Action

ID	RefReader	PortOut	Elapse	RefTime
1	10	1	25	0
2	11	1	25	0
3	12	1	0	0

Holiday

Day	RefGroup „Action-ID“	RefTime
2012-05-01	1	3
2012-05-01	2	4
2012-05-01	-3	5

In the action list above, the door module with the ID 12 was assigned the time model 2 which switches port 1 of the module. If separate holiday control has been activated in the setup, time model 2 is not applied to the relay output at May 1, 2012, but time model 5.

Extended Parameterization ZK-II

The value range of the parameter 'ActiveGeneral' has been extended by the value 8. Additionally to the general permission (value 9), a PIN request is executed - if defined so for the user and activated for the reader. Furthermore, at both configurations of the ID cards with the ActiveGeneral value 8 and 9, the validity period of the ID card is checked.

For ZK-II the operation modes online, offline or online/offline after time-out are available. In online mode, configuration lists stored in the device are not considered. A data record is read from the server, analyzed and an action triggered. In offline mode, the configuration lists of the terminal are used to grant or deny access to a person. Online / offline after time-out is a combination. If the server is unavailable, the terminal can decide on basis of its lists whether to grant access to a person or not.

Timing of the Digital Outputs for the MasterIV Device Series:

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

The following tables must be configured:

- ▶ Action
- ▶ Reader
- ▶ Time

Description:

Each action that is to be activated must be entered in the table Action. The table Action refers to the tables Reader and Time. In the table Reader the module is provided on which the relay or the Open Collector is to be switched. The reference to the table Time indicates when the switch is to 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 is only to 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 output 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 PZE-MasterIV.
- ▶ The heating system is to be set to the "day mode" at **07.00** am and to 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	TimeEnd	TimeEnd
3	12345	10:00	00:00
4	12345	16:00	00:00
5	1234567	07:00	19:00

Action.txt

ID	RefReader	PortOut	Elapse	RefTime
6	1	1	15	3
7	1	1	15	4
8	2	1	0	5

5.7.2. Description of Tables for Access Control 2

Table **Reader** (List of all devices installed in the system)

Name	Data type	Length	Description
ID	Number (int)	4	Unique Key (value>0) of the Reader table.
ZM	Number (int)	4	In our example, it has number 1. If there are several PZE-MasterIVs 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. If several RS485 bus lines are used on a device, each additional line must be entered with Master ID + 1.
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 or RS485 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 by which a person without a card gets access.

Table **Identification** (list of all devices installed in the system - master and door modules)

Name	Data type	Length	Description
ID	Text (ASCII)	20	Contains the ID card no. which is read at the TMR33 device or terminal. An ID card can occur several times (is assigned to several authority groups).
Group	Number (int)	4	Assigns the ID card to an authority group.
Pin	Number (int)	8	Activates a PIN request if not equal 0. Please note that a PIN must not start with 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 analyzed by software developed for this purpose and sets off the alarm.
ActiveStart	Text (Date)	10	The tag entered here indicates the start date of the validity of the ID card. (for example 2007-07-12 = yyyy-mm-dd)
ActiveEnd	Text (Date)	10	The tag entered here indicates the end date of the validity of the ID card. (for example 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; field ID are now only a PIN for access. 4 = pin = threat code i.e. the threat code is used instead of the Pin entered. 5 = The value for Duress / threat code is not transferred to the PIN adds up to form the threat code (ex: Pin = 1234, Duress = 1 -> threat code = 1235; Pin = 1234, Duress = 6 -> threat code = 1230) 6 = permanent opening for U & Z cylinders 7 = Burglary alarm system, allowed to switch on/off 8 = general authority (with PIN request) 9 = general authority (no PIN request)

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

Identifier	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 for which entering an additional PIN is not necessary (at peak times etc.).

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

Name	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 (form: 7 digits at most 1-7 e.g. 134567 = Monday, Wednesday till Sunday)
TimeStart	Text (Time)	5	The start point for the period of time. (form: 24h HH:MM)
TimeEnd	Text (Time)	5	The end point for the period of time.

Table Holiday (setting blocking days like holidays or company holidays)

Name	Data type	Length	Description
Day	Text (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. Zero defines a global validity for all groups.
RefTime	Text (Time)	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 Event (assigning an action to a signal at the digital input)

Name	Data type	Length	Description
RefReader	Number (int)	4	Module (door module or master) where the digital input is.
PortIn	Number (char)	1	Number of the digital input on the module. Possible values: 1 ... 9 & A ... W corresponds to port 1-32 (digital in)
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 **Action** (list of all workable actions in the access control system; an action group, i.e. all actions with the same action number, can switch several relays)

Name	Data type	Length	Description
ID	Number (int)	4	Action number, it can occur several times due to 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 (char)	1	Indicates the number of the output on the module. Possible values: 1 ... 9 & A ... W corresponds to port 1-32 (digital out)
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) This is a function to switch relays directly via time (table) Please not mix this function with the normal access actions. !!! By a time-table setting "1234567 00:00-23:59" is the relay permanent on.

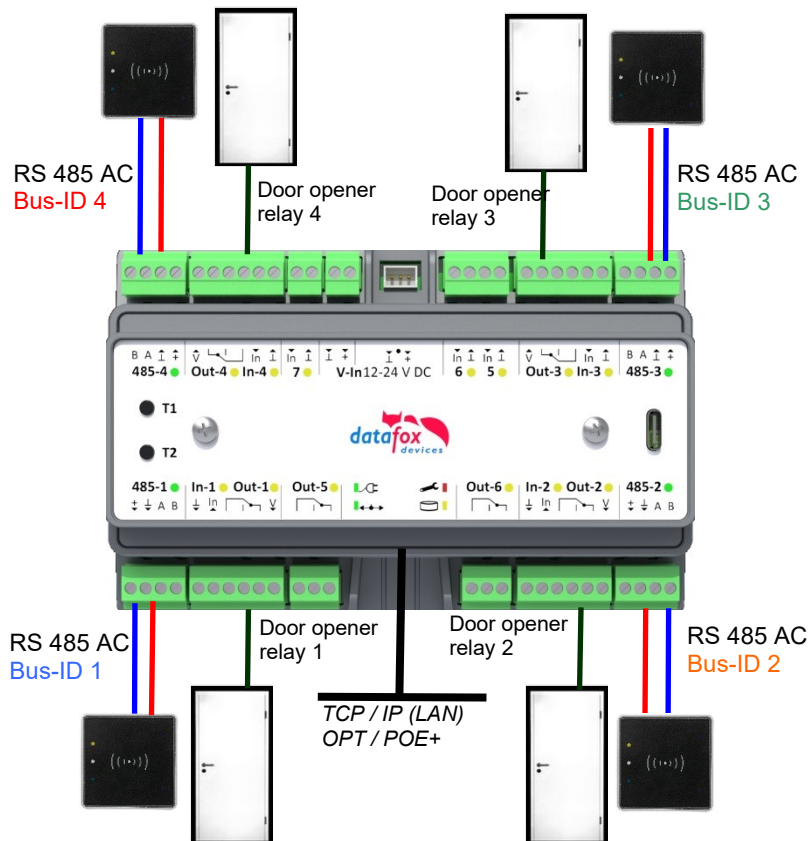
5.7.3. Wiring variants for the KYO Fourloc

The KYO Fourloc can be optionally equipped with up to 4 access control bus connections RS485. This results in a variety of connection variants for setting up an access control system.

5.7.3.1. Wiring in a star form of the access control for the KYO Fourloc

Wiring plan for 4 Doors, 4 relays in the KYO Fourloc:

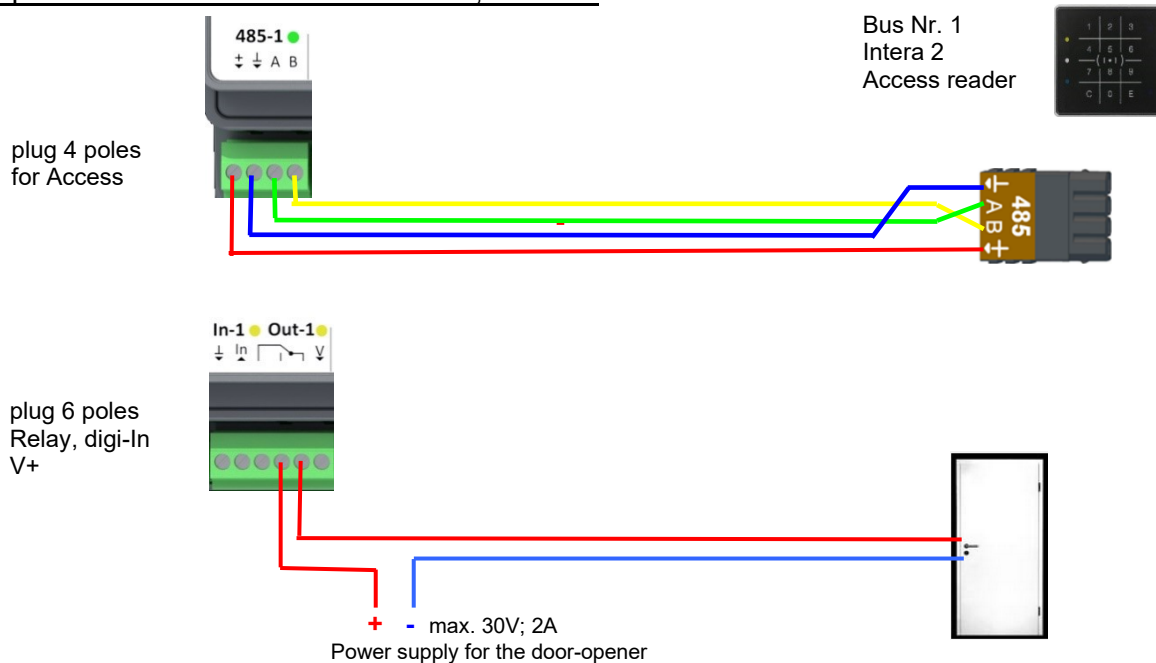
! Recommend for new installations.



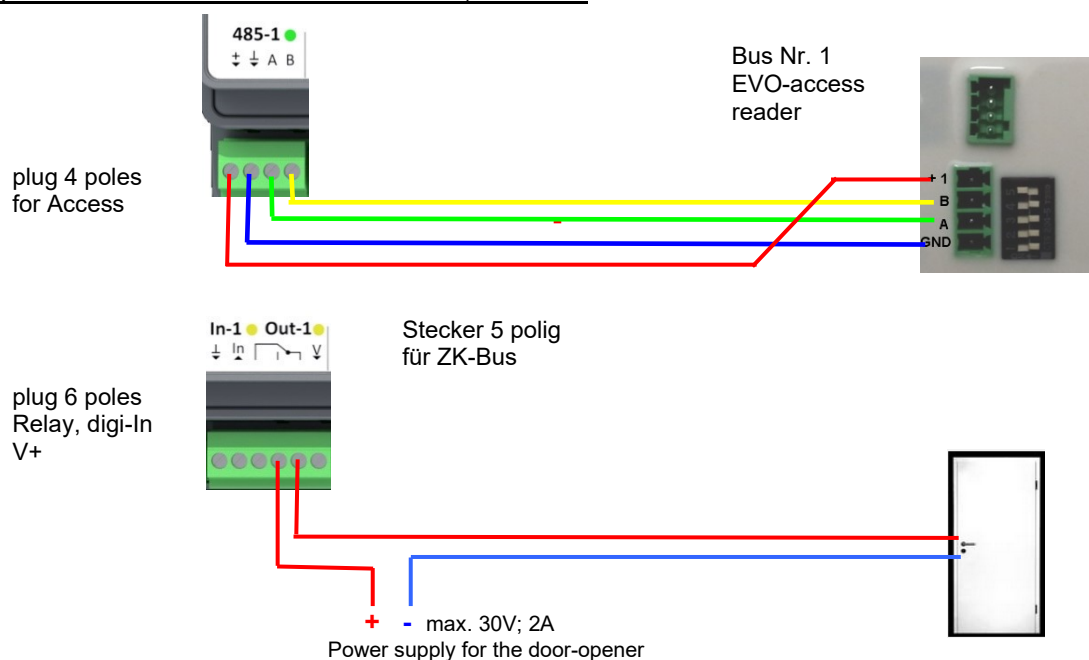
Example for Reader Table,

ID	ZM / Bus-ID	TM (Busadresse)	RefLocation	RefAction	PinGeneral	Beschreibungstext
1	1	010	1	1	0	Reader on RS485 Bus ID 1
2	2	010	2	2	0	Reader on RS485 Bus ID 2
3	3	010	3	3	0	Reader on RS485 Bus ID 3
3	4	010	4	4	0	Reader on RS485 Bus ID 4
4	1	320	0	1	0	KYO Fourloc V4 (Mastergerät)

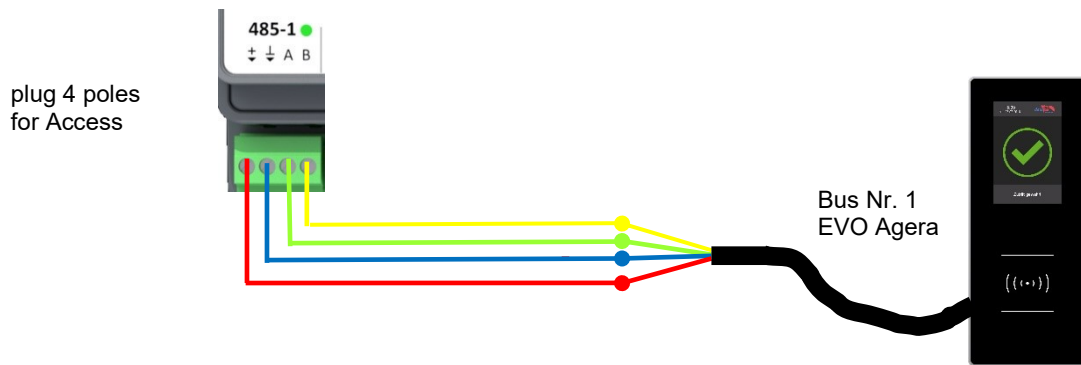
Wireplan for one of the 4 access-reader; Intera 2:



Wireplan for one of the 4 access-reader; Intera 1:



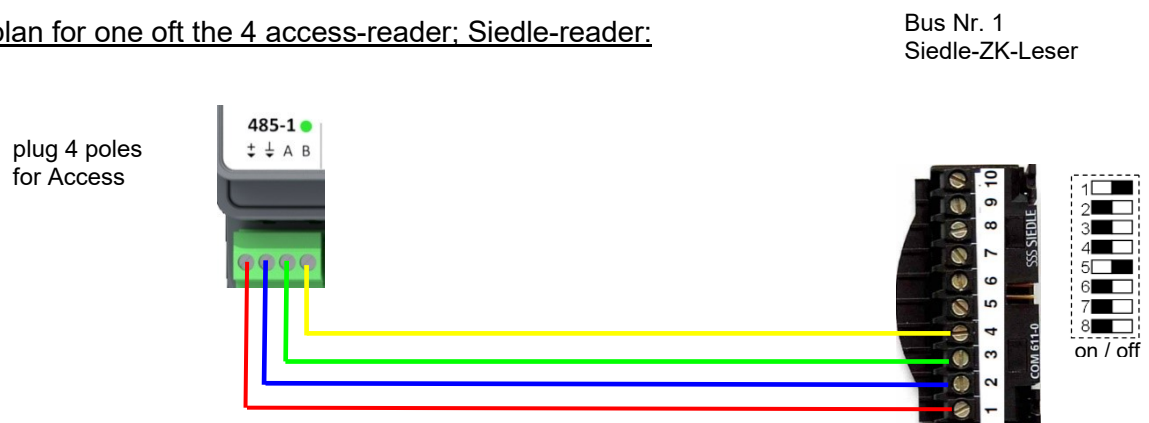
Wireplan for one of the 4 access-reader; EVO Agera:



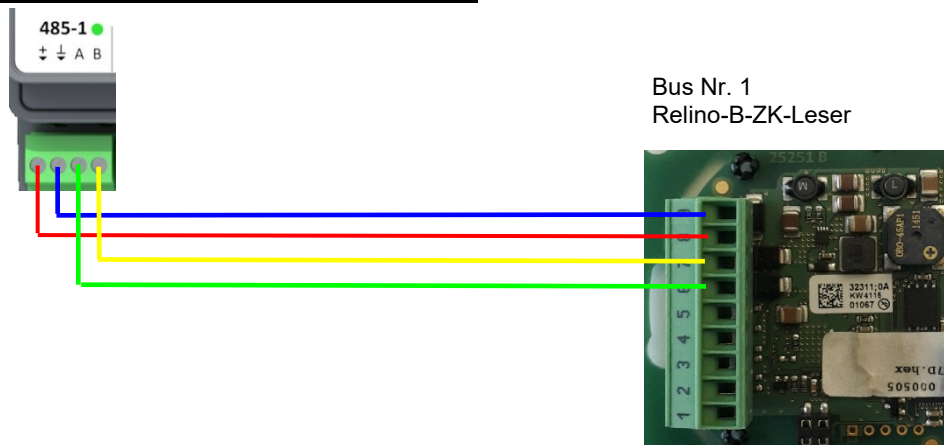
Wireplan for one of the 4 access-reader; PHG-reader:



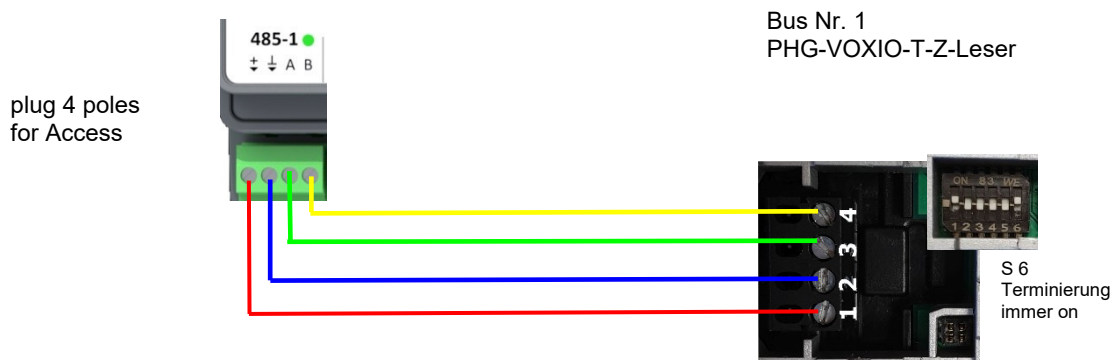
Wireplan for one of the 4 access-reader; Siedle-reader:



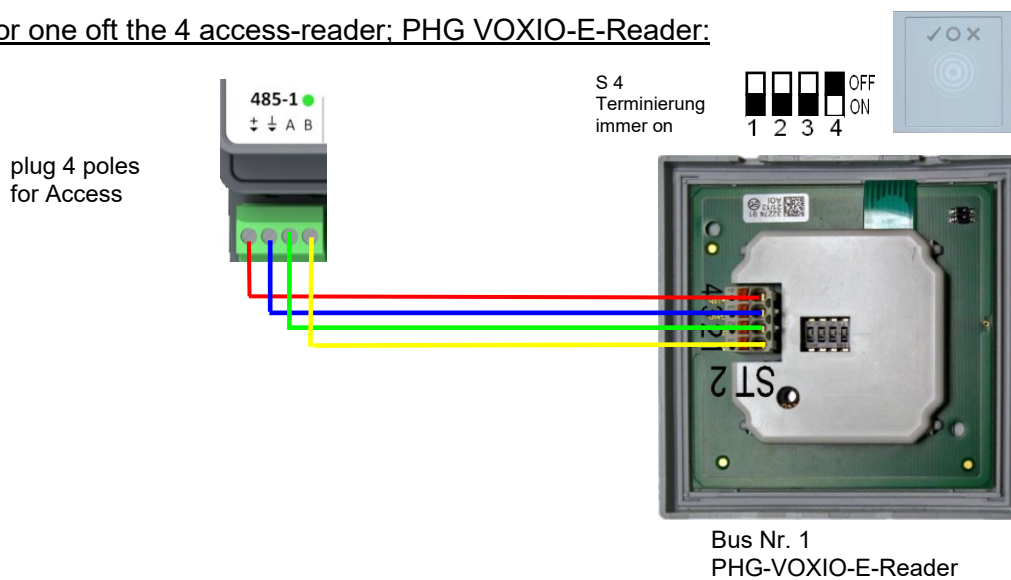
Wireplan for one off the 4 access-reader; PHG Relino-reader:



Wireplan for one off the 4 access-reader; PHG VOXIO-T-Z-Reader:

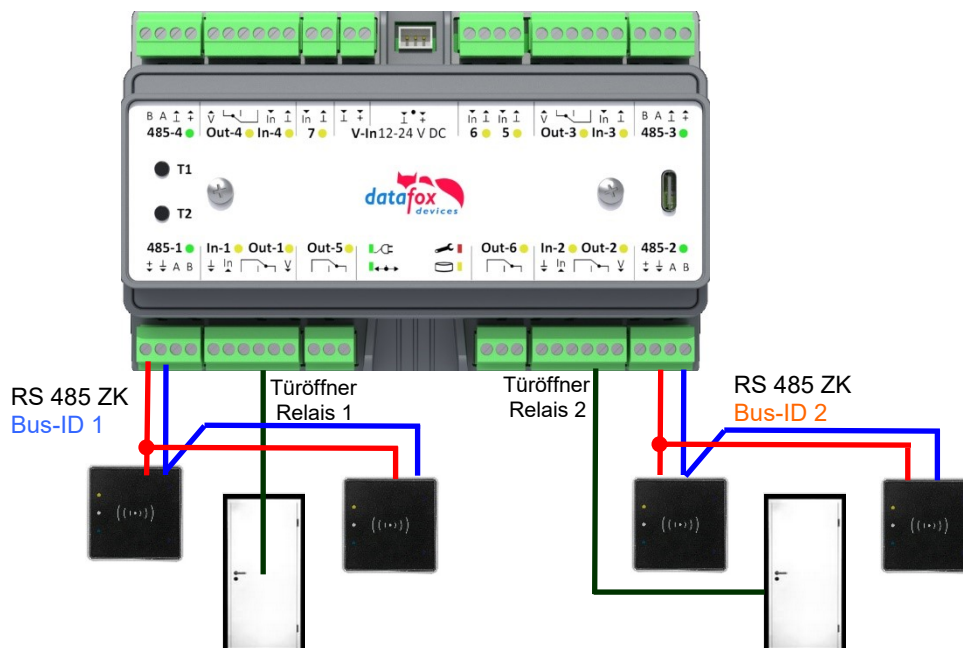


Wireplan for one off the 4 access-reader; PHG VOXIO-E-Reader:



5.7.3.2. Two doors, 4 access-reader

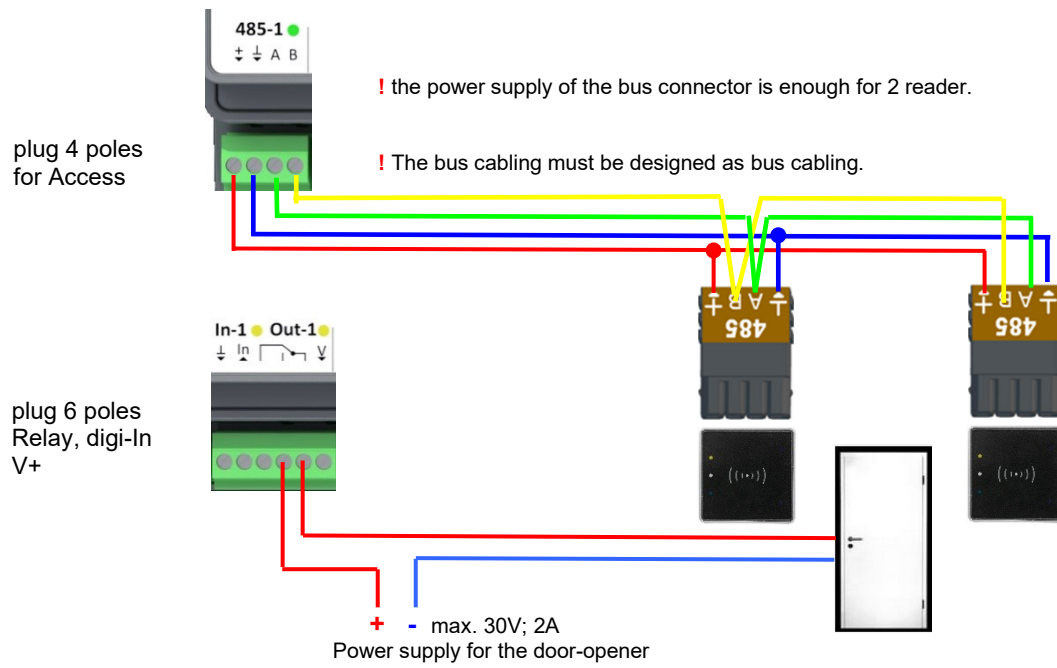
Cable plan for 2 doors, 2 relays KYO Fourloc:



Reader table for this example:

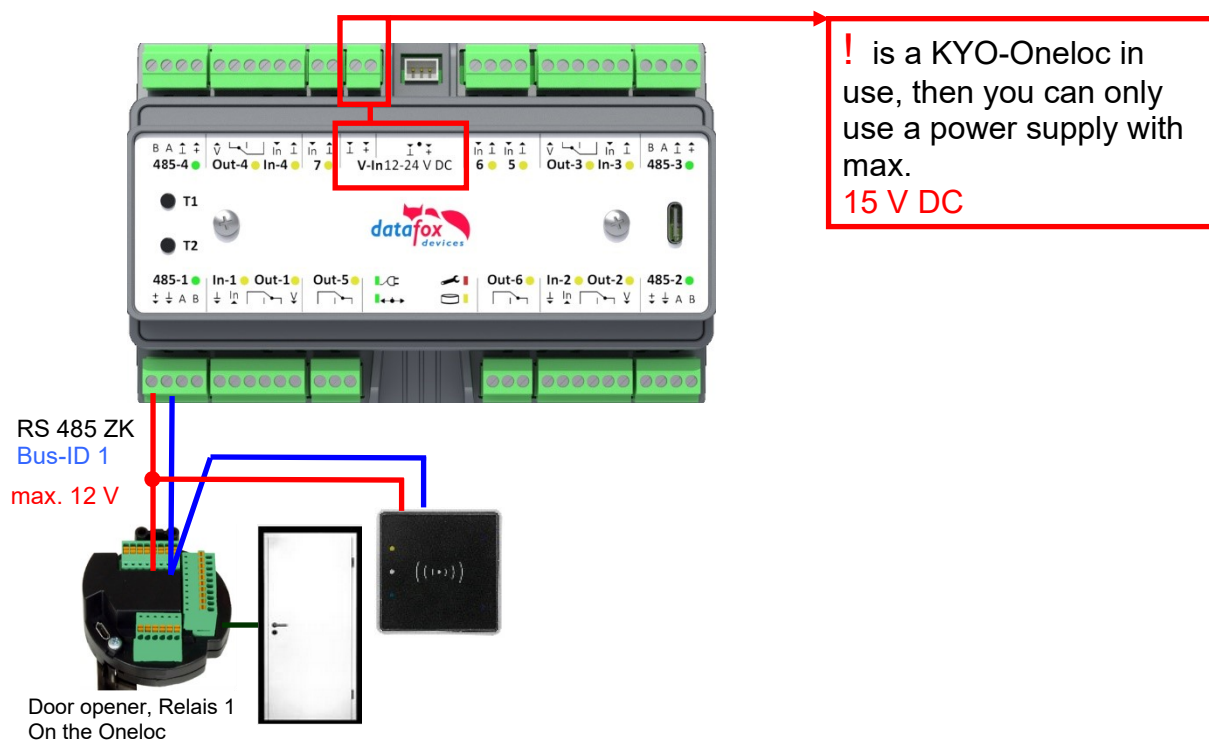
ID	ZM / Bus-ID	TM (Busadresse)	RefLocation	RefAction	PinGeneral	Beschreibungstext
1	1	010	1	1	0	Leser / RS485 Busadresse 1 / Bus ID 1
2	1	020	2	2	0	Leser / RS485 Busadresse 2 / Bus ID 1
3	2	010	3	3	0	Leser / RS485 Busadresse 1 / Bus ID 2
4	2	020	4	4	0	Leser / RS485 Busadresse 2 / Bus ID 2
6	1	320	0	1	0	KYO Fourloc V4 (Mastergerät)

Wireplan for 1 Door, 1 Relay, 2 access reader, EVO Intera II:

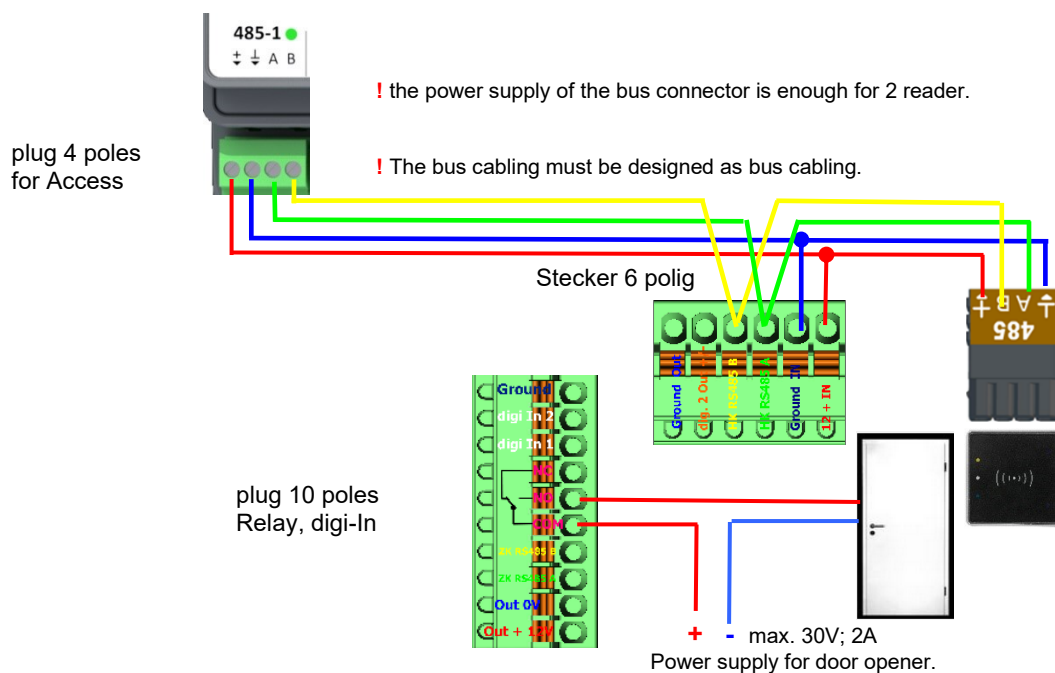


1.1.1.1 Cable plan for KYO-Oneloc and Intera 2 access reader

Cable plan for 1 reader, 1 Oneloc as an relay in the Busline KYO Fourloc:



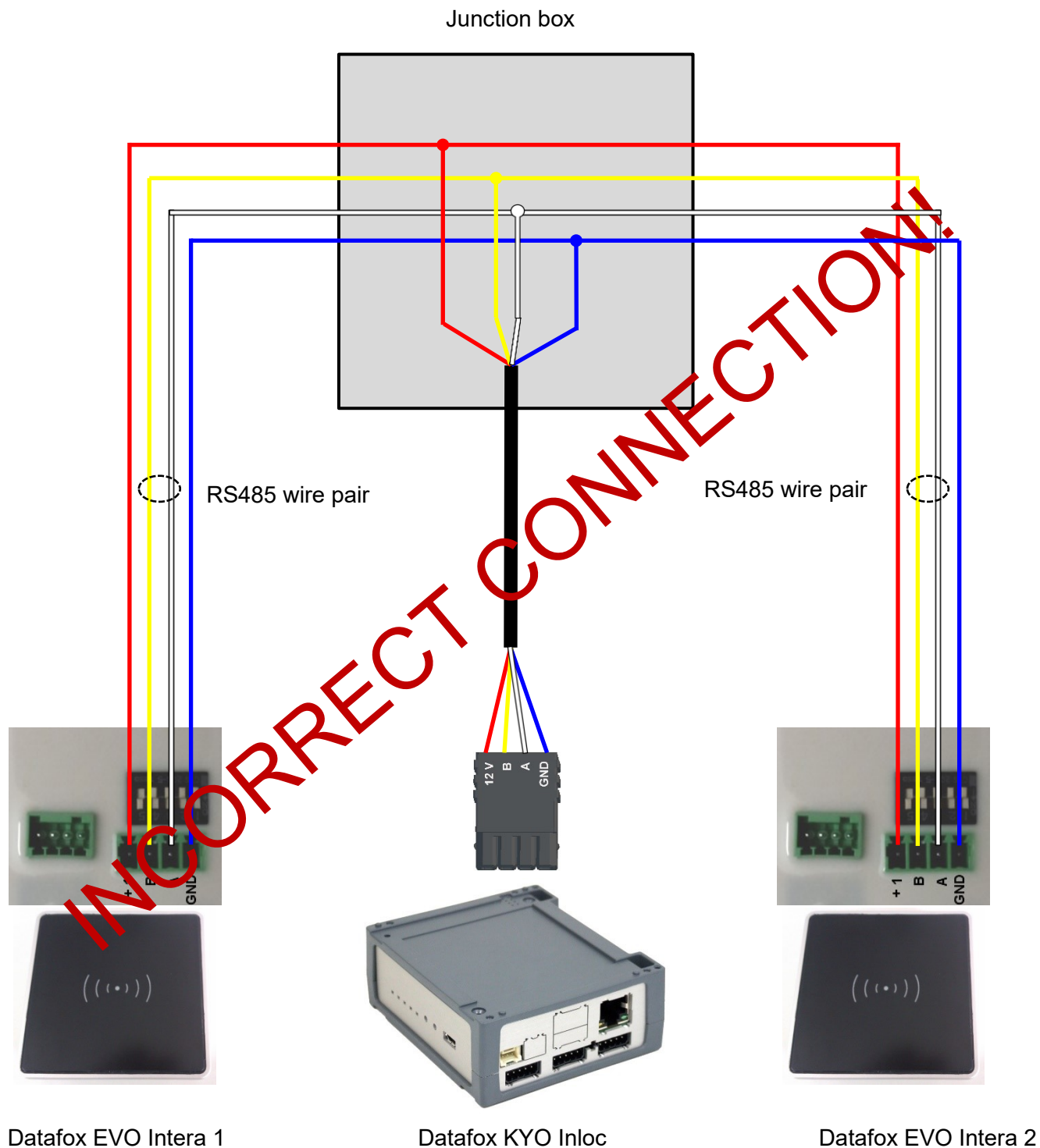
Wireplan for 1 Door, 1 Oneloc / Relay, 1 accessreader, EVO Intera II:



5.7.4. Instructions for the electrician for installing the access control system

5.7.4.1. Star-shaped bus wiring

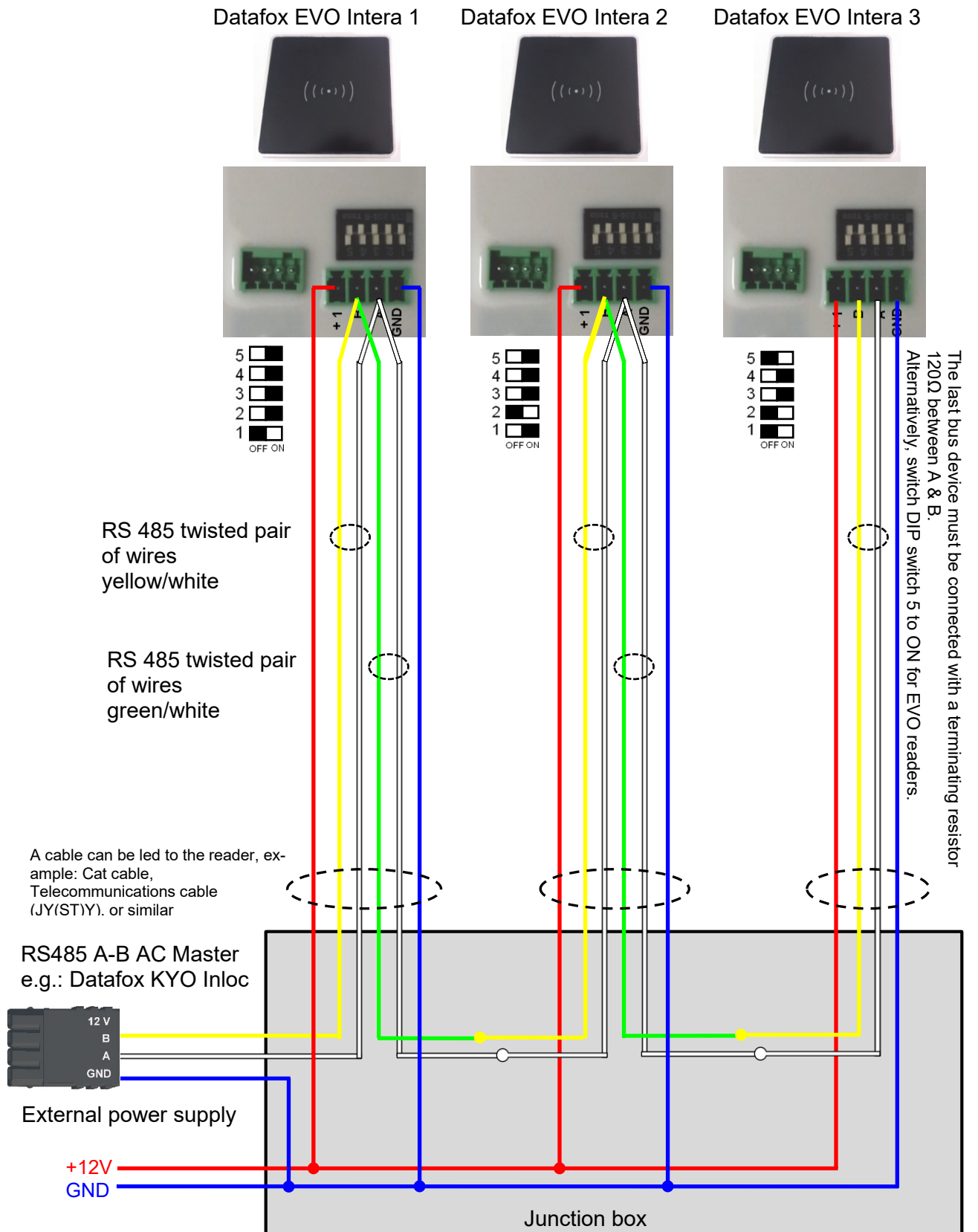
**! Incorrect star connection of the RS485 bus.
RS485 wire pairs must not be connected in parallel.**



Correct!

Correct bus wiring of the access readers with star-shaped cable routing.

The wiring must not be parallel from one point. The wire pairs A and B must each be routed in series directly to the terminal of a reader and from there on to the next bus device in order to ensure smooth operation of the bus communication.



5.7.5. Access-control with Intera 2

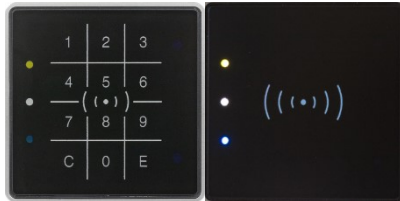
The following hardware is available to set up an access control intera 2 modules. The devices can be combined in different ways according to their hardware requirements.

KYO Fourloc

If the device MasterIV is used for access control, door supervision or remote monitoring, one device can supervise up to 8/16 doors.

EVO Intera

with PIN and without PIN

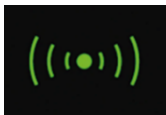


dimensions: 81 x 81 x 19 mm (wxhxd)

The EVO Intera access reader can be used with 125 kHz, 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 visualizing the state, a buzzer for the acoustic signaling and a proximity sensor.



Backlight signaling:
Glowing white = reader ready for use
Flashing white = reader not recognized



Backlight signaling:
green = access allowed



Backlight signaling:
red = Access denied or reader is currently being configured by the master. Or Reader was recognized but not entered in the reader.



LED – **Yellow** RFID-Tac in the field

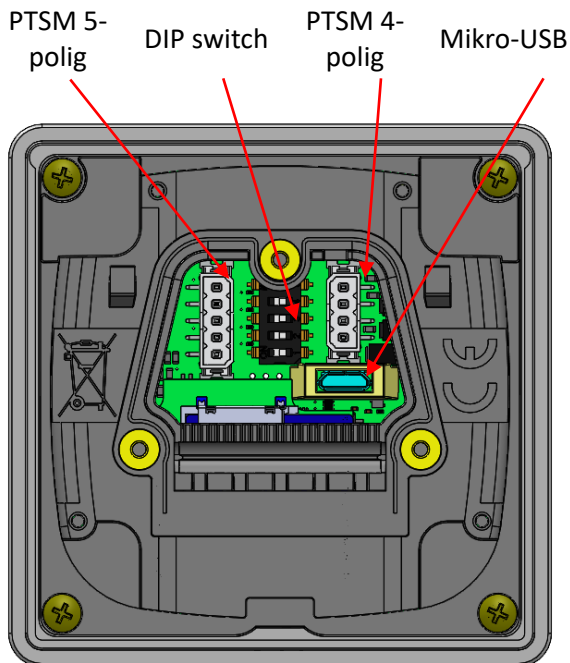
LED – **white** = sleepmode (deactivated via proximity sensor.)

LED – off -> ready to read and the background LED is on.

LED – **Blau** (no function)

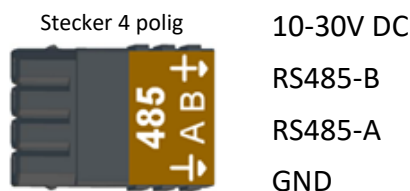
Anschlussbelegung:

Anschlussbelegung



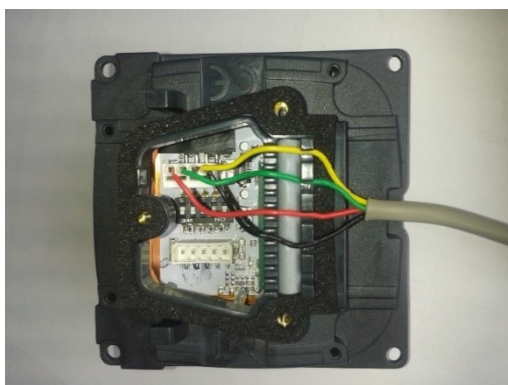
Anschluss an die PTSM Steckverbinder Connection to the PTSM connector

The EVO Intera II is supplied with the 4-pin or 5-pin mating connector for connecting the reader. These are protected against polarity reversal and are supplied by Datafox with printed assignment.



DIP - Schalter	Off	On
1 – Adresse Bit 0	+ 0	+ 1
2 – Adresse Bit 1	+ 0	+ 2
3 – Adresse Bit 2	+ 0	+ 4
4 – Adresse Bit 3	+ 0	+ 8
5 – end resistor 120R	no-activ	activ

Beispiel	5-4-3-2-1
Adress 2, with active end resistor	1-0-0-1-0
Adress 3, no active end resistor	0-0-0-1-1

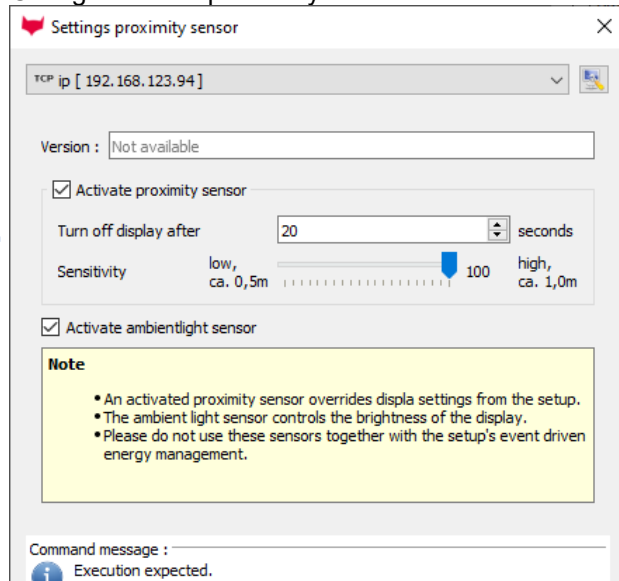
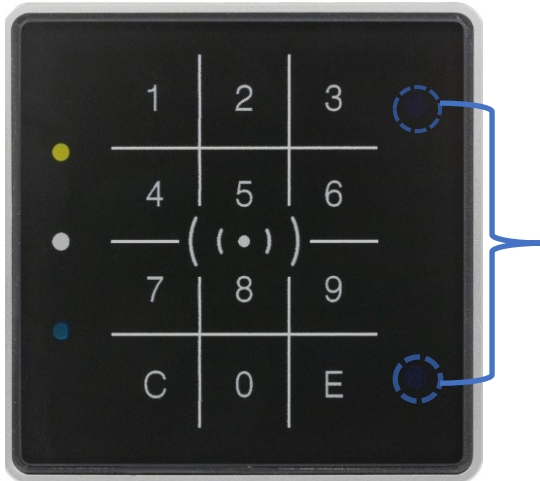


wiring

The EVO Intera II has an integrated cable comb to accommodate single wires up to $d=1.5\text{mm}$ incl. suspension for strain relief. Lay the cores as shown.

Settings for proximity sensor:

The proximity sensor are on righth side on the reader:
The settings are include in the SW DatafoxStudioIV Configuration -> proximity-sensor:

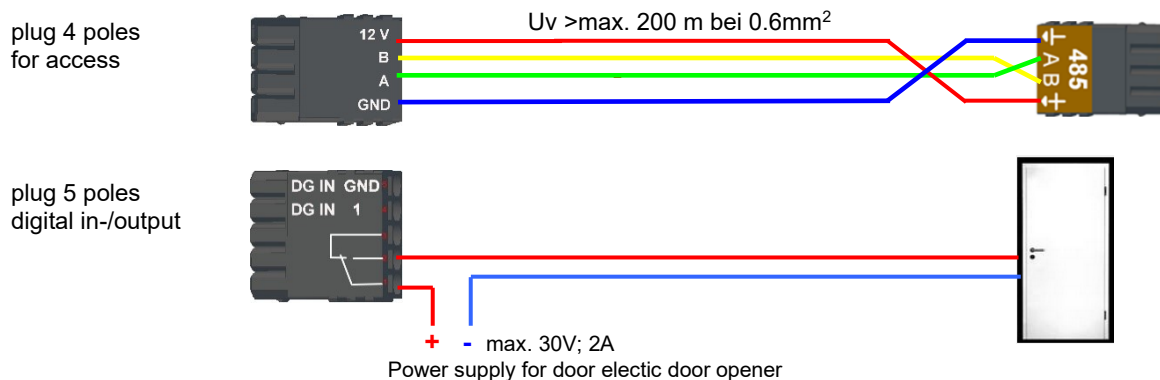


example Reader Table,:

ID	ZM / Bus-ID	TM (Busadresse)	RefLocation	RefAction	PinGeneral	Beschreibungstext
1	1	010	1	1	0	Leser an RS485 Modulplatz 1 = Bus ID 1
4	1	320	0	1	0	ZK-Box V4 (Mastergerät)

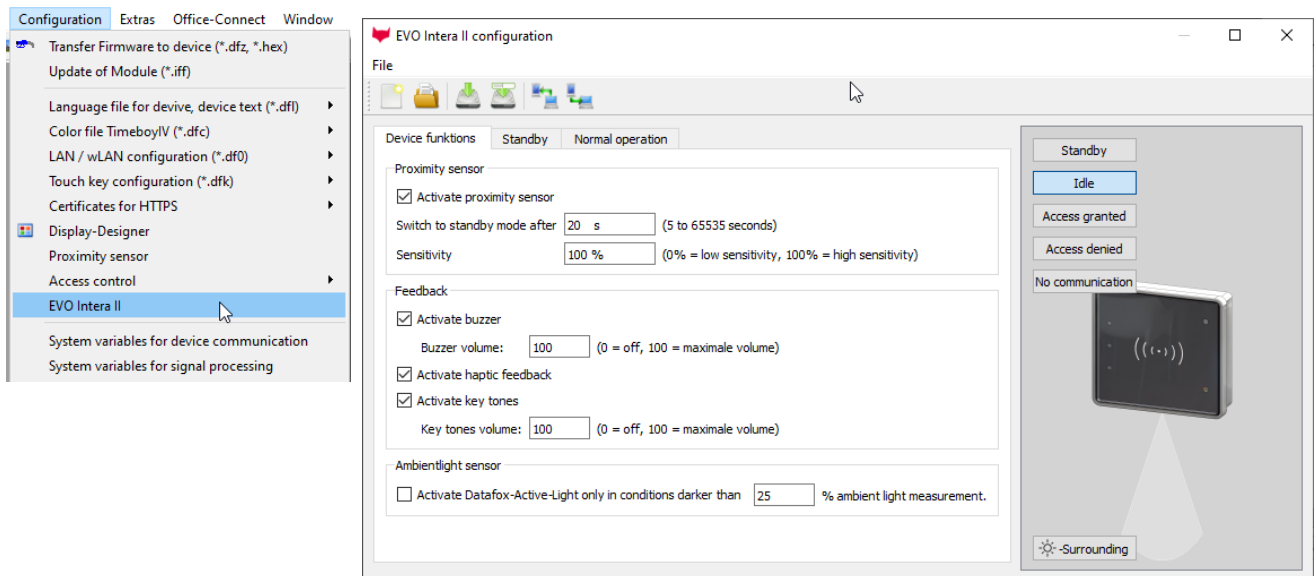
wire plan for one reader, Intera 2:

Bus Nr. 1
EVO-ZK-Leser



5.7.5.1. EVO Inter II, Individual settings

The mask for setting the EVO Inter II configuration can be accessed in the Datafox Studio via the configuration menu:



The mask allows setting / adapting the behavior of the EVO Inter II. These settings are divided into 3 areas:

- Configuration of the device sensors and actuators (device functions tab))
- Configuration of the standby configuration (sub-configuration of the proximity sensor)
- Configuration of normal operation (Standard Operation tab)

In addition, a preview of the reader signaling is shown based on a selected operating status.

5.7.5.2. Functionality of the EVO Inter II

The EVO Inter II is an RFID reader for use in access control. As such, it is designed for operation on an RS485 bus and uses the phg_crypt communication protocol, which is used as a de facto standard in large parts of the industry.

The reader differs from many competing products in terms of its features:

- It can project indirect lighting
- It has sensors for ambient light and proximity detection.
- It can be used as a pin reader and then generate haptic feedback in addition to the acoustic feedback.

The EVO Inter II also has three programmable LEDs on the left. Functions can be assigned to these LEDs, such as signaling an ID in the field of the RFID reader or a person nearby. There are also other functions such as permanently on / off or switched by the access controller.

The Datafox Studio dialog described in this chapter is used to set up these features. The configuration is transferred via the USB interface of the reader.

5.7.5.3. Global function

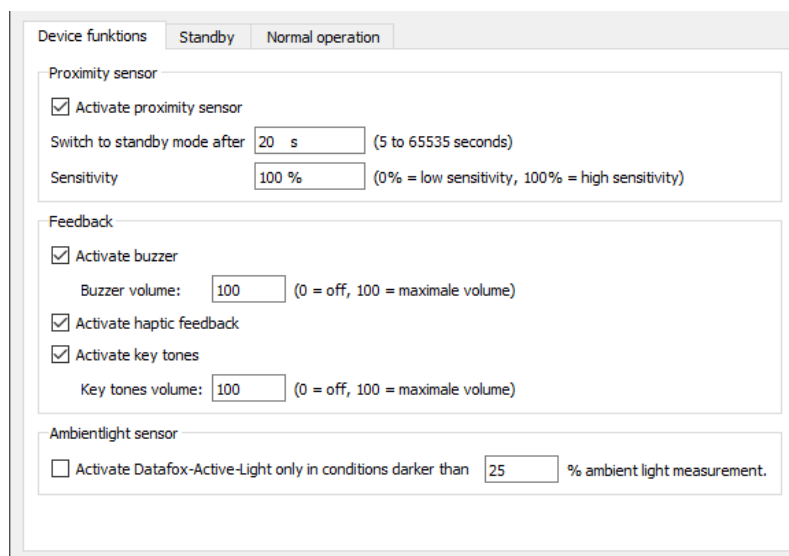


From left to right, the mask offers functions for

- Creation of a new standard configuration
- Reading in a configuration file
- Save the configuration file
- Save the configuration file under a new name
- Transfer of the configuration file to an EVO Intera II
- Reading the configuration file from an EVO Intera II

These actions are also available from the File menu.

5.7.5.4. Einstellung der Gerätefunktionen



The EVO Intera II has a proximity sensor - if this is activated, the standby lighting can be set. The standby mode is activated if no person is detected in the vicinity of the reader for an adjustable period of time (20 seconds as standard).

Depending on the structural situation, it may be necessary to limit the sensitivity of the proximity sensor, for example if it is used in narrow aisles and the opposite wall is supposedly recognized as a person nearby.

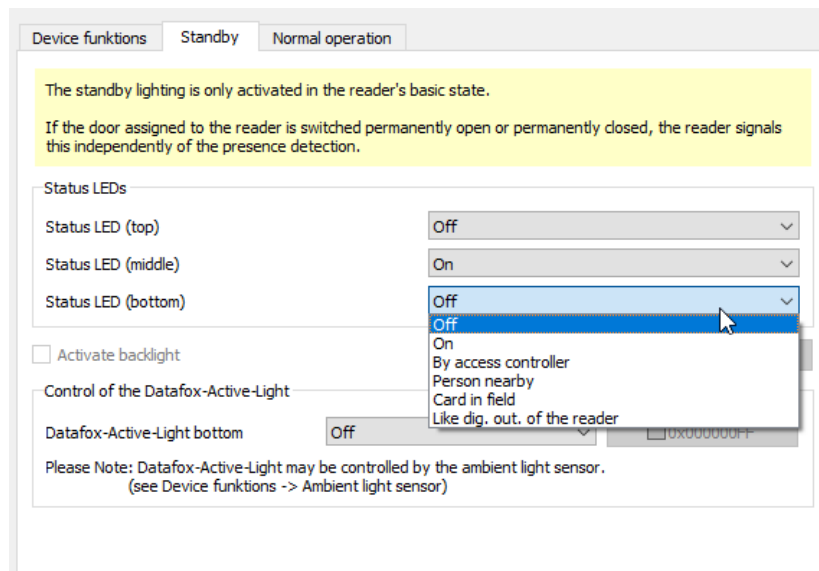
As feedback are next to the

- Buzzer for access events still
- Haptic and sound feedback ready for PIN readers.

You can set the maximum volume for all acoustic feedback so that the reader can also be adapted to quiet office environments.

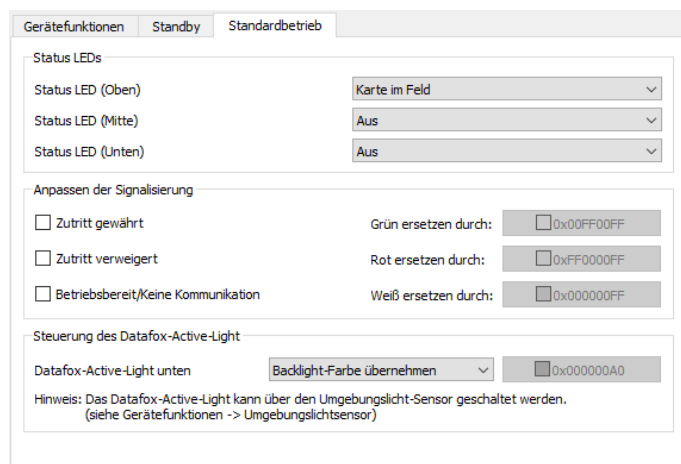
The reader can adjust its brightness - e.g. in order not to shine too brightly at night - to the brightness of the surroundings. If this function is desired, activate the ambient light sensor.

5.7.5.5. Settings for standby



The standby mode of the EVO Intera II is activated if the proximity sensor has not detected a person in the vicinity for an adjustable period. In this operating mode, the 3 LEDs can be assigned functions that differ from the normal operating mode. In addition, the Datafox Active Light can be switched if it is built into the reader.

5.7.5.6. Setting for standard operation

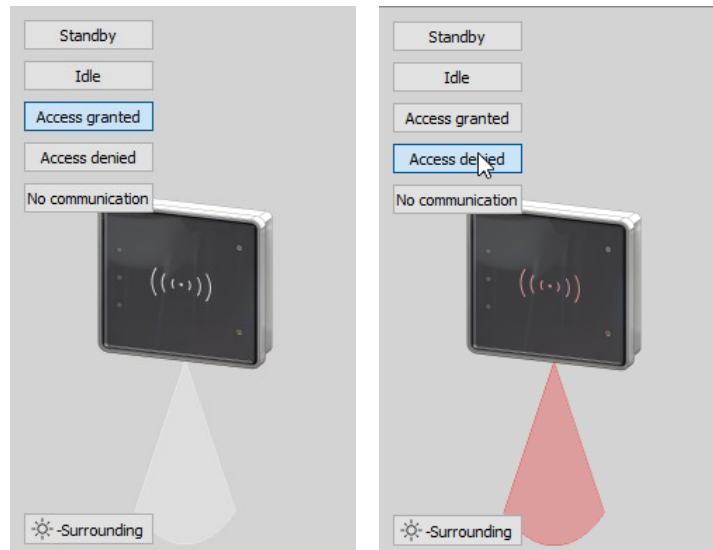


In standard operation, the EVO Intera II fulfills the normal functions of an access reader - the reader is controlled via the access bus by an access controller. In the simplest case, the reader transmits the read RFID data to the access controller and is then switched to access granted ("green") or access denied ("red"). If no access signaling is active, the reader normally lights up white.

In addition to assigning functions to the three programmable LEDs, you can adjust the colors used for green, red and white. You can also - if built into the device - set the color and brightness of the Datafox Active-Light.

5.7.5.7. Preview of reader behavior

An EVO Intera II is shown on the right-hand side of the configuration mask. This changes - based on the currently loaded configuration - its appearance. Use one of the five buttons to select the operating status to be displayed.

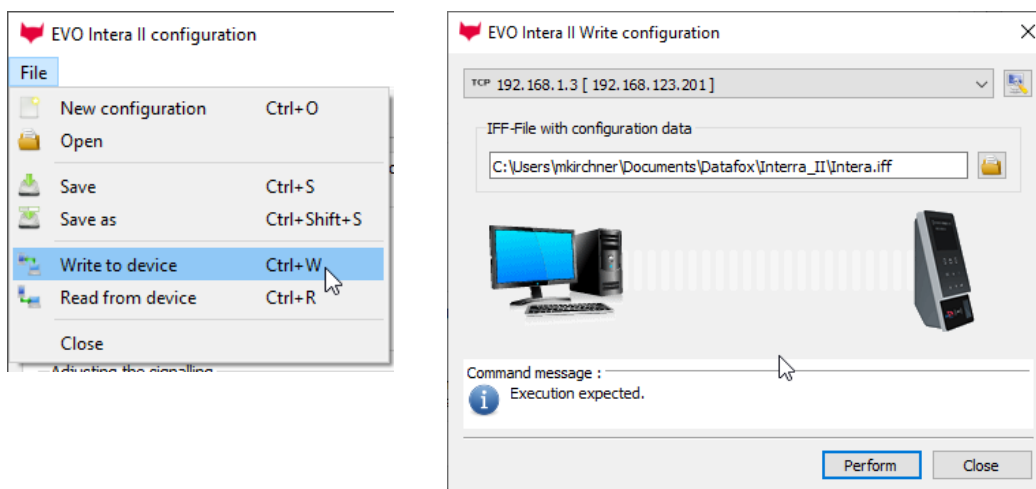


„Zutritt gewährt“ und „Zutritt verweigert“ mit Datafox Active-Light im Modus „Backlight-Farbe übernehmen“

You can use the button at the bottom left in the preview area to explicitly switch the reader to day or night operating mode.

5.7.5.8. Transfer to the device

To transfer to or from a reader, please connect it to your PC via USB. After pressing one of the buttons for transfer, you will see the file transfer dialog of the Datafox Studio:



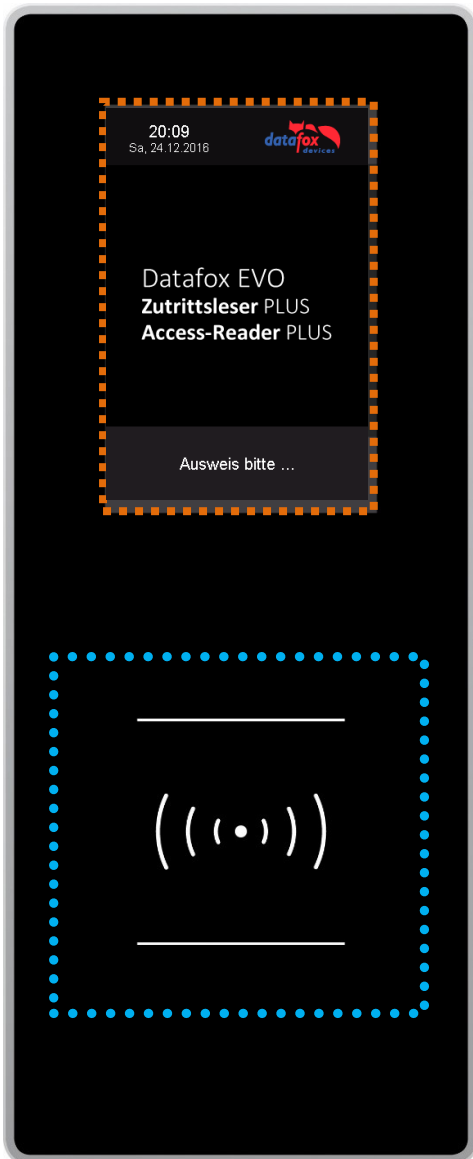
Here you can select the configuration file to be transferred - the version opened in the editor is the standard assignment of the transfer dialog via the transfer button to the device. By pressing the "Execute" button, the configuration file is transmitted to the reader (or read from there).

5.7.6. Access control II with EVO Agera

5.7.6.1. Display and operation

The reader has a capacitive touch.

All images displayed by the reader and marked as standard below can be exchanged.



Display:
The entire display area is backed by a touch screen.

With the DatafoxStudioIV, images can be stored here for a gallery display and for the necessary inputs/outputs.
See → Configuration → Display Designer.

Reading range of the transponder with backlight in RGB colours.
The control of the LED is controlled exclusively by the readers firmware.

Access denied = red -

Access permitted = green -

Bios activated = blue -

5.7.6.2. Display for state of access control

Currently there are 2 displayed states for:

granted access:

access denied:



Datafox standard image



Datafox standard image

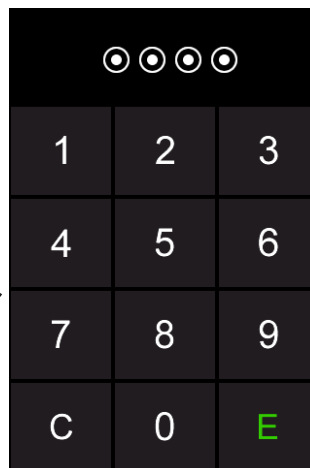
5.7.6.3. Display the number keypad

If an additional PIN is requested for access, the keypad will be displayed automatically. For access only by entering a PIN, it is sufficient to briefly touch the display to activate the PIN display.

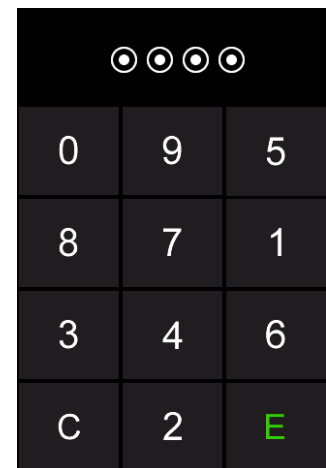


Datafox standard image
Picture 1 of the gallery

tapping



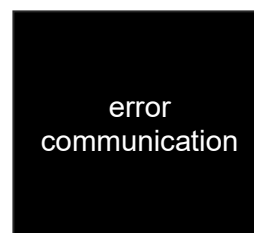
Datafox standard image
PIN normal



Datafox standard image
PIN randomization

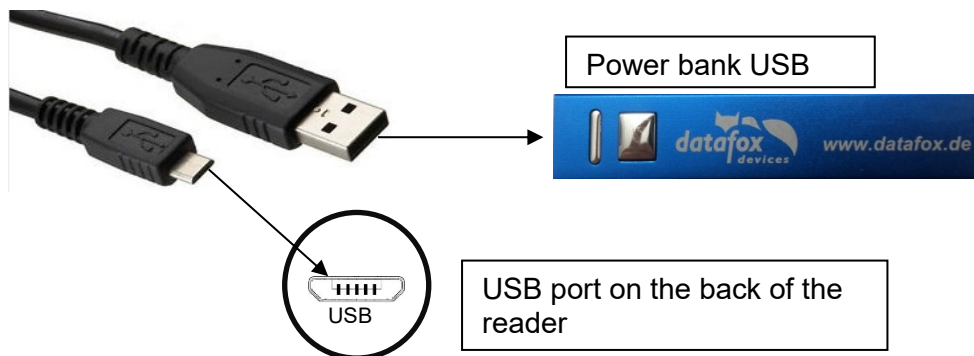
5.7.6.4. Error message

The reader is in constant communication with the master. If communication is interrupted, this is indicated by the text "Communication error" on the reader.

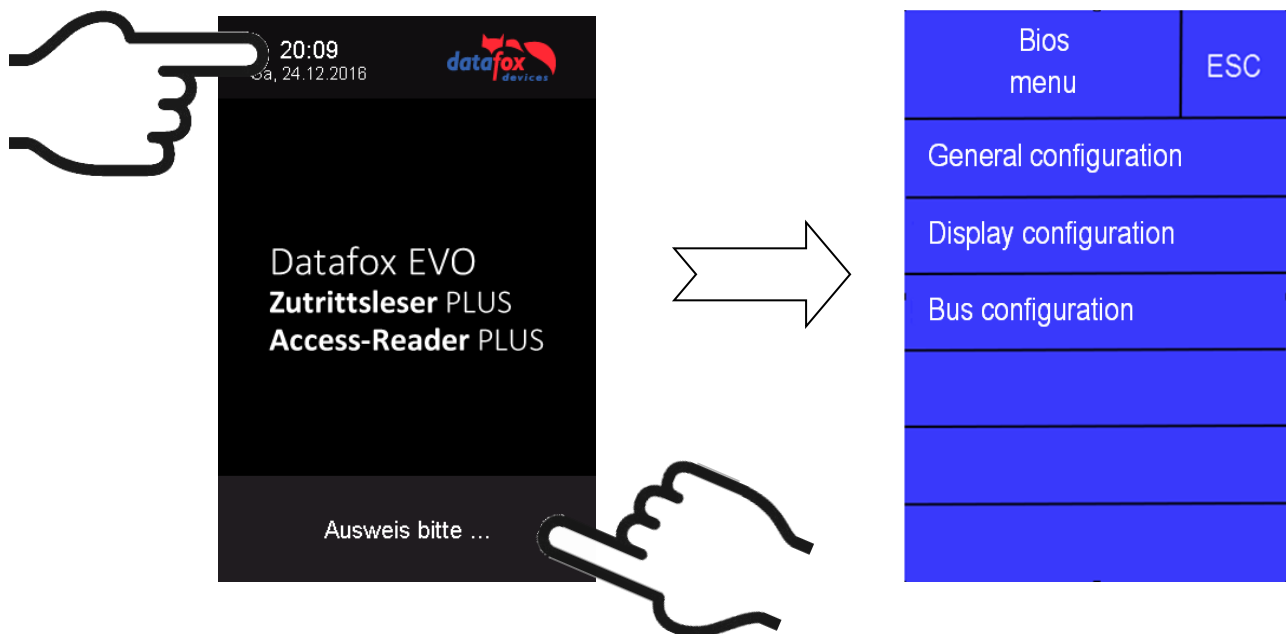


5.7.6.5. Bios-menu

Connect the reader to the 12V power supply with the connecting cable.
 As soon as it is started, connect the reader via USB to a PC or a small battery (power bank).
The Bios menu can only be accessed when the USB port is powered.



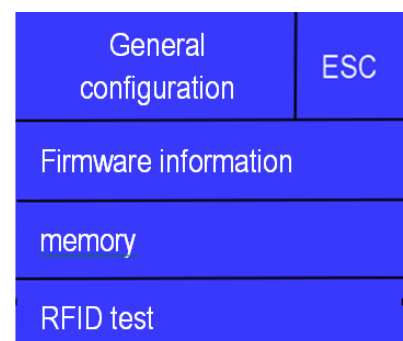
Tap both top left and bottom right at the same time.



5.7.6.6. General configuration

The following information can be called up in the general configuration:

- Installed firmware, serial number
- Memory allocation for the image memory
- Transponder test for the transponder configured in the master setup.



5.7.6.7. Display configuration

The following parameters can be set in the display configuration:

- The brightness of the device
- Random number keys - arrangement of the pin and keyboard
- The basic activation of the pin - keyboard

Display configuration	ESC
Brightness	100%
Random keyboard	
Display Touch Pin	

5.7.6.8. Bus configuration

In the bus configuration, the initial parameters that are used for the setup of the reader must be set.

Bus Configuration	ESC
Bus number	
End resistor	

5.7.6.9. Setting the bus address of the reader for RS485 bus

The bus address is defined in the bus configuration under "Bus number".

Note that only bus addresses between 1 and 16 are possible.

The input of the bus number is confirmed with the "Enter" key (bottom right).

With the Escape button (bottom left) the process can be aborted.

Bus Nummer		
0		
1	2	3
4	5	6
7	8	9
ESC	0	↵
	←	

5.7.6.10. Activate the termination resistor of the bus

The bus terminating resistor of 120 Ω is switched on or off in the bus configuration under "Terminating resistor".

Note: If it is the last or only reader in the RS485 bus, the terminating resistor must be switched on.

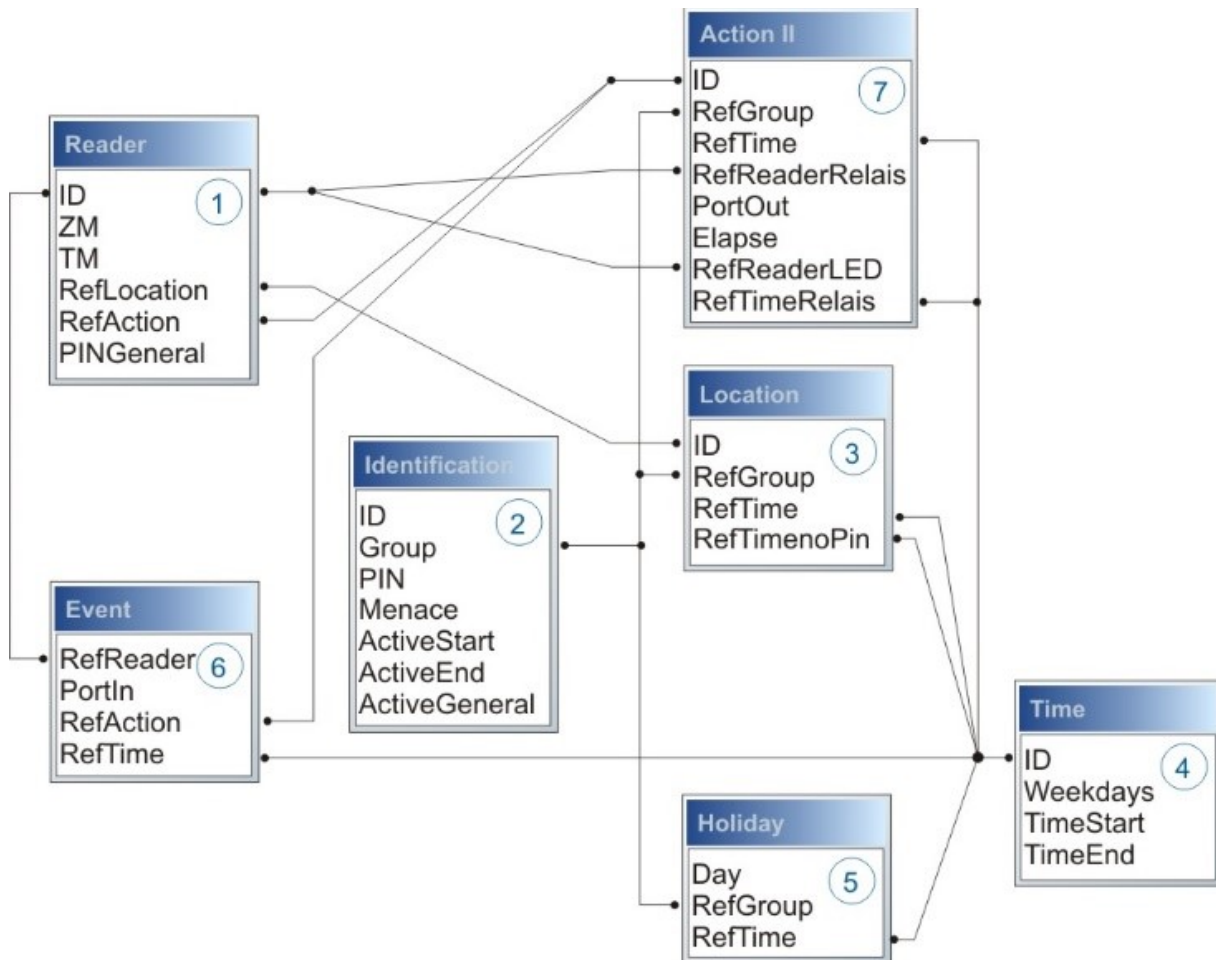
End resistor	ESC
On	
Off	

5.7.7. Function extension for access control II

5.7.7.1. General description

The access control has been extended to some functionality. To the table "Action 2" was introduced. This table replaces the previously known "Action". On the end of this chapter you find a description for the table „Action2“. Due to a lot of additional references many scenarios are now possible.

The entire logic of the access control lies in the links between the access lists. Here is an overview of the links between the access lists:



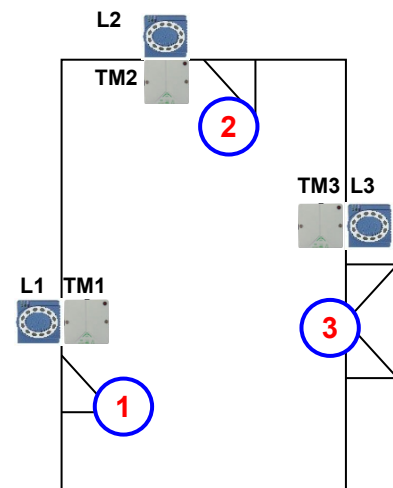
The following example gives an overview:

5.7.7.2. Examples

Example - Garage:

The facility manager comes in the morning at 7.00 o'clock and uses the Entry 1.

- with his RFID-chip he opens the door 1 for 5 seconds.
- with the same action he gives the door 3 free, the opening is now possible with a switch, until 4 o'clock pm.
- entry 2 is now open until 4 o'clock pm for the other person.
 - the closing is possible with:
 - 1 – one RFID-chip registry on group 40
 - 2 – double read of a normal RFID-chip
 - 3 - Automatic at 4 o'clock pm (define in the time table, see in row 2 „RefTime“)



Construct of Reader-, Location-, Action2- and Identification-table looks maybe at follows

Table Reader

ID	ZM	TM	RefLocation	RefAction	PinGeneral	Description text
1	1	320	0	0	0	Master device
2	1	010	100	0	0	Door-module on RS485 wire (TM1) only relays include Need not a listing in the table „action“
3	1	011	100	1000	0	RFID-reader on RS232 wire (L1) only reader All readings of RFID on this reader make all actions in the table „action“, with the ID 1000.ID 1000.
4	1	020	200	0	0	Door-module on RS485 wire (TM2) only relays include Need not a listing in the table „action“
5	1	021	200	2000	0	RFID-reader on RS232 wire (L2) only reader All readings of RFID on this reader make all actions in the table „action“, with the ID 2000.
6	1	030	300	0	0	Door-module on RS485 wire (TM3) only relays include Need not a listing in the table „action“
7	1	031	300	3000	0	RFID-reader on RS232 wire (L3) only reader All readings of RFID on this reader make all actions in the table „action“, with the ID 3000.

Table Time

ID	Weekdays	TimeStart	TimeEnd	Description text
1	1234567	00:01	23:59	24hours opening possible
2	1234567	07:00	16:00	Time for special action

Table Action2

ID	RefGroup	RefTime	RefReader Relais	PortOut	Elapse	RefReader LED	RefTime Relais	Description
Read an RFID chip on reader 1								
1000	10	0	2	1	5	3	0	Opening normal for 5s. Group (10; 20; 30) have always entrance
1000	20	0	2	1	5	3	0	
1000	30	0	2	1	5	3	0	
1000	30	2	4	1	32400	5	0	door 2 open for 9h (max. 16:00)
1000	30	2	6	1	32400	7	0	door 2 open for 9h (max. 16:00)
1000	40	0	2	1	-1	3	0	command door open, return
1000	40	0	4	1	-1	5	0	command door open, return
Read an RFID chip on reader 2								
2000	10	0	4	1	5	5	0	Opening normal for 5s. Group (10; 20; 30) have always entrance
2000	20	0	4	1	5	5	0	
2000	30	0	4	1	5	5	0	
2000	30	2	4	1	32400	5	0	door 3 open for 9h (max. 16:00)
2000	30	2	6	1	32400	7	0	door 3 open for 9h (max. 16:00)
2000	40	0	4	1	-1	5	0	command door open, return
2000	40	0	6	1	-1	7	0	command door open, return
Read an RFID chip on reader 3								
3000	0	0	6	1	5	0	0	This action is for all Groups are listed in the table "Location".

Table Location

ID	refGroup	refTime	refTimeNoPin	Description
100	10	1	0	Group 10, 20, 30 and 40 have access on this reader.
100	20	1	0	
100	30	1	0	
100	40	1	0	
200	10	1	0	Group 20 can not use this entrance 2.
200	30	1	0	
200	40	1	0	
300	10	1	0	The Master of Garage and the facility manager can open this door.
300	30	1	0	

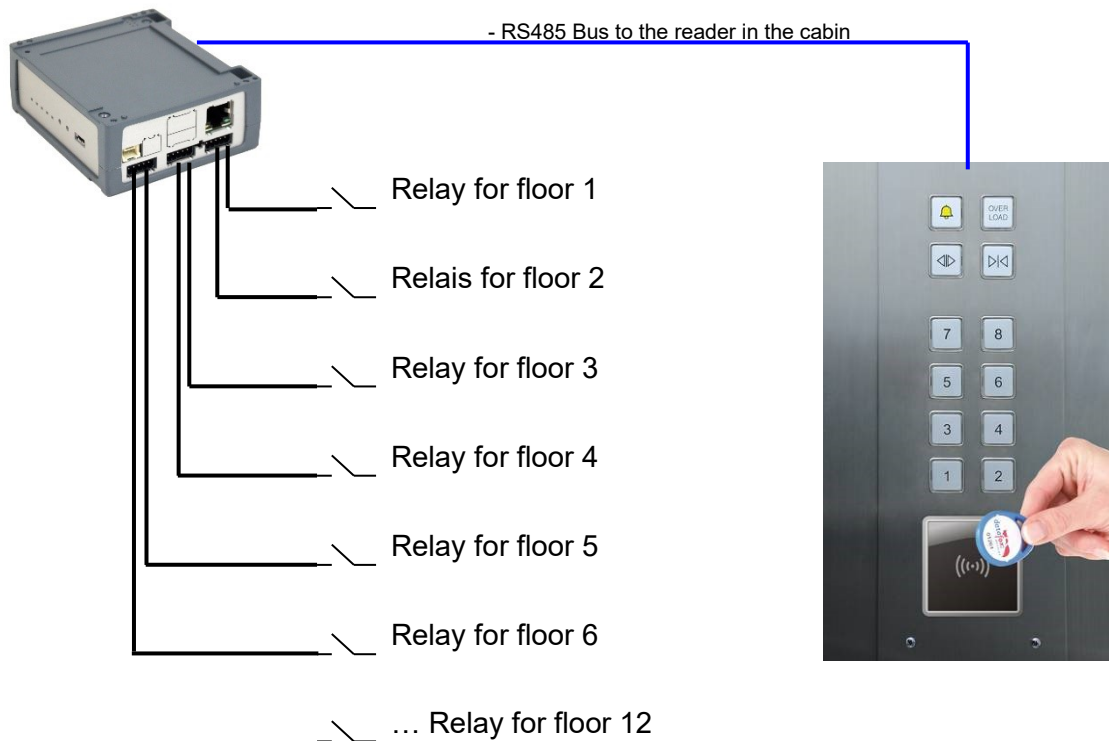
Table Identification

ID	Group	Pin	Menace	ActiveStart	ActiveEnd	Active	Description
1111	10	0	0	2005-01-01	2015-12-31	1	Master of Garage
2222	20	0	0	2005-01-01	2015-12-31	1	Skilled workers
3333	30	0	0	2005-01-01	2015-12-31	1	Facility manager
4444	40	0	0	2005-01-01	2015-12-31	1	Facility manager second RFID-chip, only for closing the door

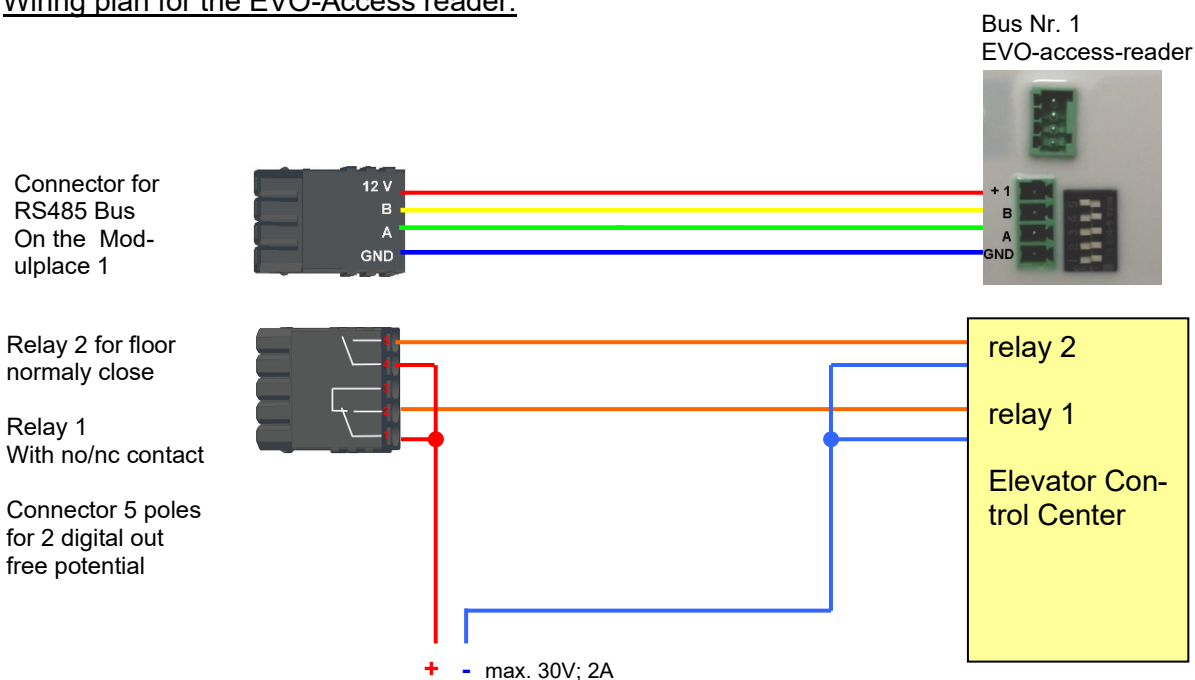
Example - elevator

The goal is to allow users only to exit at the allowed floor.
Then tenant uses the transponder to activate only the switch for his floor.

In the cabin of the elevator the RFID-reader is installed. The Datafox-Device is on the top of the cabin.



Wiring plan for the EVO-Access reader:



The content of Reader-, Location-, Action2- and Identification- might look like follow:

Table Reader

ID	ZM	TM	RefLocation	RefAction	PinGeneral	Description
1	1	320	0	0	0	Master device
2	1	000	100	1000	0	Reader on RS485 wire

Table Action2

ID	RefGroup	RefTime	RefReader Relais	PortOut	Elapse	RefReader LED	RefTime Relais	Description
Buchungen am Leser in der Kabine								
1000	10	0	1	1	20	2	0	Group 10 only for floor 1.
1000	20	0	1	2	20	2	0	Group 20 only for floor 2.
1000	30	0	1	3	20	2	0	Group 30 only for floor 3.
1000	40	0	1	4	20	2	0	Group 40 only for floor 4.
1000	50	0	1	5	20	2	0	Group 50 only for floor 5.
1000	60	0	1	6	20	2	0	Group 60 only for floor 6.
1000	102	0	1	1	20	2	0	Group 102 moving to floor 1 and 2
1000	102	0	1	2	20	2	0	
1000	104	0	1	1	20	2	0	Group moving to floor 1, 2 and 3.
1000	104	0	1	2	20	2	0	
1000	104	0	1	3	20	2	0	

Table Location

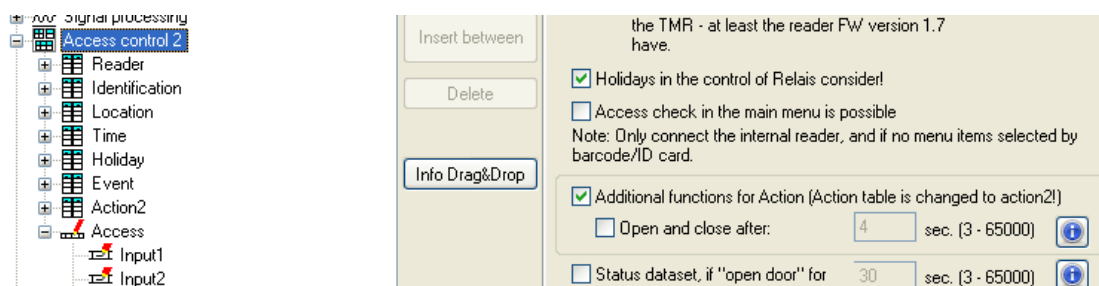
ID	refGroup	refTime	refTimeNoPin	Note
100	10	1	0	All Groups 10, 20, 30, 40, 50, 60,102 and 104 must listed in the location for this reader.
100	20	1	0	
100	30	1	0	
100	40	1	0	
100	50	1	0	
100	60	1	0	
100	102	1	0	
100	104	1	0	

Table Identification

ID	Group	Pin	Menace	ActiveStart	ActiveEnd	Active	Description
1111	10	0	0	2005-01-01	2099-12-31	1	Tenant of an apartment on the floor 1
2222	20	0	0	2005-01-01	2099-12-31	1	Tenant of an apartment on the floor 2
3333	30	0	0	2005-01-01	2099-12-31	1	Tenant of an apartment on the floor 3
4444	40	0	0	2005-01-01	2099-12-31	1	Tenant of an apartment on the floor 4
5555	50	0	0	2005-01-01	2099-12-31	1	Tenant of an apartment on the floor 5
6666	60	0	0	2005-01-01	2099-12-31	1	Tenant of an apartment on the floor 6
1102	102	0	0	2005-01-01	2099-12-31	1	Tenant of an apartment on the floor 1 and 2
1104	104	0	0	2005-01-01	2099-12-31	1	Tenant of an apartment on the floor 1, 2 and 3

5.7.7.3. Description of the table „Action2“

The switching from „Action“ to „Action2“ it's a setting in the StudioIV.



Name	Data type	Length	Description
ID	Number (int)	4	Action number, it can occur several times due to several actions that have to be worked through.
RefGroup	Number (int)	4	Only work this action for the listed Group. 0 = for all groups work this action.
RefTime	Number (int)	4	Give a time, and only works this action to this time. (0 = works ever) ! Not mixed with times in RefTimeRelais!
RefReader Relais	Number (int)	4	Reference to the list reader, action to switch a relay on this listed reader in table reader.
PortOut	Number (char)	1	Indicates the number of the output on the module. Possible values: 1 ... 9 & A ... W corresponds to port 1-32 (digital out)
Elapse	Number (int)	6	Specifies the period of time a relay is switched ! The time is in seconds! When (-1) is specified, the relays are reset directly. With (0) the relays switch for the duration specified for the relay with RefTime. "FRA" activates Free Access "BLA" activates Blocked Access = permanent red signal "STD" returns to Standard mode.= Deactivate from FRA or BLA
RefReaderLED	Number (int)	4	This is a reference to the table Reader to switch the LED on other modules
RefTimeRelais (only for auto-automatic time switch)	Number (int)	4	The time model indicates when the output may be switched. (0 = not used). (Automatic time control) ! Action how here work with automatic times, be not mixed with action from the access!



Caution:

By transferring the table "Action 2" to the unit, the table "action" is replaced. Thus, only entries in the table "Action 2" will be considered.



Caution:

If you would like to continue working with the "action" table, the table "Action 2" may not be transferred to the device.
A table "Action 2" has already been transferred to the device, it must be cleared by loading a new setup.

5.7.7.4. Additional functions for Access Control

All functions described below are only supported in conjunction with the Action 2 table.

Possible functions:

- Logging, in an internal list, in which room each employee is located.
- Hard antipassback
- Soft antipassback (= only the software is informed that an ID card has entered a room 2 times = status message 251)
- BDS
- Type associated to the supervised door unctinality.

The table "ReaderProps" must be created under the table structure of the operation:

Name	Data type	Length	Description
RefReader	Number (int)	4	Reference to the ID of the Reader whose properties should be specified
Type	Number (int)	2	Type of the Property 1 = anti-passback 2 = BDS-System 3 = BDS 4 = BDS 5 = Type associated to the supervised door unctinality.
Mode	Number (int)	1	Mode for details of the type above 1 - Only protocol the attendance of persons in a room (in list "presence"). 2 - Hard anti-passback (no entry when conflict detected, status code 250) 3 - Soft anti-passback (entry allowed when conflict detected, status code 251).
Duration	Number (int)	10	Access is permitted again after the duration time has elapsed. Value in seconds. 0 = no end time. It is necessary to enter another room necessarily

The table "ReaderProps" is created in the setup:

Protocol - Function

Essentially serves to ensure that when several access managers are used, they know in which room a person is located.

Via your software, this information is distributed between the access managers or can be read out if required.

See the documentation DFComDLL

- DFCTable.....
- DFCPresence....

Soft antipassback

A status message 251 is issued here if one and the same badge enters the same room more than once. Admission is still permitted!

Hard antipassback

A reader is always assigned to a room. This room may then only be entered once with the same ID. If the same ID card is used again for access to this room, it will be rejected. Status 250 is output in the data record during access control.

Here you can choose whether the reject is limited in time or whether Hard remains active.

In the case of Hard Active, access is not permitted again until another room ID has been accessed. This corresponds to leaving the previous room.

5.7.7.5. List Presence

This list is created by the access controller itself.

This makes it possible to enable the tracking of people and rooms via several access controllers.

If the Antipassback function is to be used via several access controllers, this list must always be updated by the software to all access controllers.

Example:

A room (example room ID 10) has several doors that are managed by different access control boxes. If a person enters this room, an entry is created in the Presence list of this box that this person is in the room.

The other access control boxes can now also be informed that the person with ID X is in room 10. To do this, an entry in the Presence list must be created in the other boxes via your software (with DLL).

This is done using the method [DFCTableAppendRowData](#) Append Data Row to the table.

The same applies if a person leaves the room, this entry must be deleted in the Other Access Control Boxes.

Name	Data type	Length	Description
ID	Number (int)	20	ID of the person that is stored in the presence list.
RefLocation	Number (int)	4	Reference to the ID of the room, defined in the table "Location", where this person currently stays
TimeStamp	Number (int)	10	Time stamp when the person entered the current room Integer in seconds, starting 01.01.2000.

5.7.8. Integration of a Burglar Detection System (BDS)

Integration of a Burglar Detection System (BDS)

Starting with firmware version 04.03.12 the integration of a BDS into the access control system is possible.

You may control the state of up to five BDS sections using PIN readers and arm or disarm them.

In the presence of a BDS the access controller checks, that the BDS section is not armed. If armed, it will reject transponder events leading to opening the door of an armed section due to the armed BDS. Access transponder events will be evaluated according to the normal access control rules and only be granted if the reader is either part of no BDS section or part of a disarmed BDS section. An access control event rejected to an armed section will result in a dataset with “BDS armed” state.

You may (try to) arm or disarm a BDS section any time using a PIN reader associated to it. As second attempt to either arm or disarm a BDS section will result in “BDS already armed“ or “BDS already disarmed” status passed to dataset.

5.7.8.1. Configuring up the BDS

In order to activate the BDS inside the access control sub system, the setup list „ReaderProps“ is required. Up to now this list was required to configure “AntiPassBack” only. To configure BDS the ReaderProps requires twelve columns.



Please note:

- If you are transferring list data using the DatafoxStudioIV it is not possible to transfer “empty” columns. Please fill these columns using “0” values.
- The width of the ReaderProps’ columns may be chosen arbitrarily. However, it is important that the required information fit into the columns!

To setup the BDS three types of entries are required. Firstly the relay(s) to active the BDS is/are required as well as inputs to query the BDS’s current status. Additionally PIN readers of the access control system are required to allow activating / deactivating the BDS sections. Finally the PIN readers will have to associate to one or more BDS sections.

The sequence of the entries inside the “ReaderProps” list does not matter.

5.7.8.2. Relays and digital inputs for controlling the BDS (Type 2)

The relays associated to arming or disarming the alarm sections are set up according the entries described in this chapter. Additionally the digital input to indicate the readiness to be armed and the armed-state of the BDS section is configured here.

Column	Name I the Setup	Data type	Length	Description
1	RefReader	Number (int)	4	Not required, leave empty
2	Type	Number (int)	variable 10	Type 2 = BDS – definition entry for relay and digital input
3	Area	Number (int)	variabel max. 10	Number associated to the BDS section
4	OutArmReader	Number (int)	4	Reference to the device (controller or bus member) that contains the relay for arming the BDS.
5	OutArmPort	1-9; A...	1	Nummer den Ausgangs
6	OutUnarmReader	Number (int)	4	Reference to the device (controller or bus member) that contains the relay for disarming the BDS.
7	OutUnarmPort	1-9; A...	1	Number of the relay on the device column 6
8	InRdyReader	Number (int)	4	Reference to the device (controller or bus member) that contains the digital input that signals the BDS section to be ready to be armed (through "high" voltage level).
9	InRdyPort	1-9; A...	1	Number of the relay on the device column 8
10	InArmedReader	Number (int)	4	Reference to the device (controller or bus member) that contains the digital input signalling that the BDS section is armed (through "high" voltage level).
11	InArmedPort	1-9; A...	1	Number of the relay on the device column 8
12	OutElapse	Number (int)	4	0 -> The relay for arming / disarming is continuous active, otherwise duration of the relay's closing time in seconds.
13	Timeout for activate/deactivate	Number (int)	4	Adjustable timeout for EMA arming/disarming. If the column does not exist or the value =0, the default value of 5 seconds is applied. The value can be between 3000-30000 ms. Valid from firmware 04.03.21.08!

Description ReaderProbs für (Type=2) in- and output Definition!

Please note:



- If arming and disarming is using the same relay, the values in columns OutUnarmReader and OutUnarmPort have to be identical to OutArmReader and OutArmPort. If the relay then is closed, the BDS is meant to be armed, the opened relay indicates the disarmed BDS.
- If no digital input is set as „InRdyRead“, the BDS is considered to be ready to be armed any time.

5.7.8.3. Assigning codes for arming and disarming (Type 3)

In order to use a PIN reader for arming or disarming a BDS section the following entry is required.

Spalte	Name In the setup	Data type	Length	Description
1	RefReader	Number (int)	4	Reference (ID) to the PIN reader inside the reader
2	Type	Number (int)	variabel max. 10	Type assigned to this entry, 3 = BDS PIN code to "arming or disarming"
3	Area	Number (int)	variabel max. 10	BDS section
4	CodeOn	Number (int)	2	Code (max. 2 digits) to start arming mode. If these digits are entered, the reader starts the arming process.
5	CodeOff	Number (int)	2	Code (max. 2 digits) to start disarming mode. If these digits are entered, the reader starts the disarming process.
6	RefGroup	Number (int)	4	In order to allow arming or disarming a privileged tag has to be presented to the reader after entering the prefix code. After the tag the reader waits for a legitimation code (this field) before actually arming or disarming the BDS section (see Privileging transponders to control the BDS). If you enter "0" here, no PIN is enquired and any BDS privileged transponder may arm or disarm the BDS section.
7	Not required, leave empty			
8				
9				
10				
11				
12				

Hinweise:

Please note:



- If a reader controls more than just one BDS section, you will need one entry per BDS section.
- Operating codes are not interpreted numerically, so "0" or "00" are different prefix codes!
- If a BDS section is only to be armed or disarmed by the reader, enter a Minus "-" into the other operation's prefix code because "0" would be a valid code.
- Please ensure that no operating code is used more than once – the system behaviour is not defined then.

5.7.8.4. Associating BDS sections to readers (Type 4)

In order to be able to reject door openings when a BDS section is armed, the readers have to be associated to BDS sections.

Spalte	Name im Setup	Data type	Length	Description
1	RefReader	Number (int)	4	Reference (ID) to the reader definition in the Reader list
2	Type	Number (int)	variabel max. 10	Type assigned to this entry 4 = Association of reader and BDS section
3	Area	Number (int)	variabel max. 10	Definition of the BDS section
4	Not required, leave empty			
5				
6				
7				
8				
9				
10				
11				
12				



Please note:

- A reader may be part of more than one BDS section. Every section requires an entry inside the list ReaderProps.
- Readers not associated to any BDS section may be used to gain access any time using the normal access control rules.

5.7.8.5. Privileging transponders to control the BDS

To enable BDS control using an RFID transponder, this transponder has to be part of the Identification table. The corresponding group (see section [Assigning codes for arming and disarming \(Type 3\)](#), Column 6 „Group“) has to be entered as “Group” inside the Identification as well. Final requirement will be Column „ActiveGeneral“ to be set to „7“.

Should you require the RFID transponder to be enabled for all BDS sections, use “0” as “Group” value. This will enable the transponder to control all BDS sections, even if a “Group” is entered into the code definition (see [Assigning codes for arming and disarming \(Type 3\)](#), Column 6).

Once the operating code and “E” (Enter) have been entered at the PIN reader, the reader will start flashing red and green. Within the 5 seconds timeout a privileged RFID transponder has to be presented to the reader, then the PIN has to be entered. Depending on the validity of PIN and transponder, the BDS section will be reconfigured correspondingly (green signal) or left unchanged (red flashing three times).

Example for the table Identification:

The RFID-Number 59780 can switch the BDS-System and have standard access.

ID	Group	Pin	Duress	ActiveStart	ActiveEnd	ActiveGeneral
51044	1	0	0	2018-01-01	2099-12-31	1
59780	1	0	0	2018-01-01	2099-12-31	1
59780	8	0	0	2018-01-01	2099-12-31	7

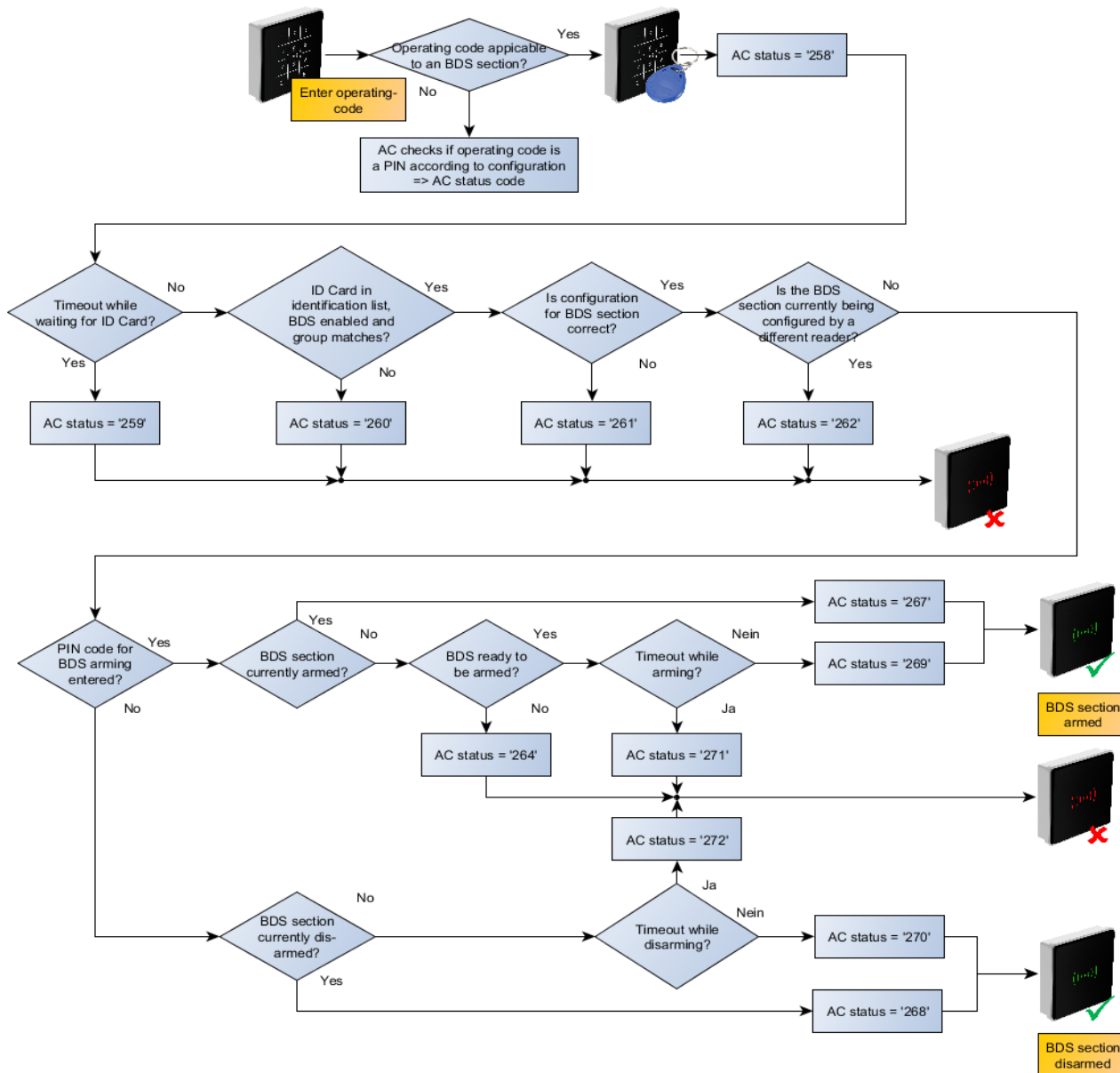
5.7.8.6. Statuscodes

The following status codes have been added in order to document the BDS state:

BSD/ EMA	Discription/ Beschreibung
258 ¹	The access control system awaits legitimation through RFID transponder and/or PIN after starting a BDS control event due to entering the operating code.
259	The access control system awaits legitimation through RFID transponder and/or PIN after starting a BDS control event due to entering the operating code.
260	During a BDS control event a non-privileged RFID transponder has been presented to the reader. This transponder is either not contained within the Identification table or does not have ActiveGeneral set to 7. See Privileging transponders to control the BDS .
261	The specified BDS section is not configured correctly.
262	There are no concurrent BDS control events supported while a BDS control event is currently being processed.
263 ¹	The BDS signals that is ready to be armed.
264 ¹	The BDS signals that is not ready to be armed.
265	The relay to arm the BDS section has been set.
266	The relay to disarm the BDS section has been set.
267	The BDS section to be armed is already armed. The reader signals "green" anyway so that the operator knows that the BDS section is armed.
268	The BDS section to be disarmed is already disarmed. The reader signals "green" anyway so that the operator knows that the BDS section is disarmed.
269 ¹	The BDS section is armed now.
270 ¹	The BDS section is disarmed now.
271	The BDS section could not be armed within five seconds. The digital input pin associated to the BDS section state still reports the section as disarmed.
272	The BDS section could not be disarmed within five seconds. The digital input pin associated to the BDS section state still reports the section as armed.
273	The access request was denied due to the BDS section being armed.
274	Identification requires an additional PIN.
275	The PIN entered does not match the stored one.
276	The PIN entered matches the stored one.
277	Timeout while waiting for the PIN to be entered.

¹) This status code contains the BDS section [1..5] as property „ID number“.

5.7.8.7. Pre-checked online processing graph



5.7.8.8. Example for the BDS integration

The following sections contains an example configuration for including a BDS:

The BDS section “2” is being configured in the example below. The AC controller’s third relay is used to request arming a section, the fourth relay of the AC controller to request disarming. Digital input 1 of the AC controller indicates that the BDS is ready to be armed. Digital input 2 of the AC controller indicates that the BDS section is currently armed.

Using the operating code “11+E” the BDS section can be armed, the code “22+E” is used to disarm the section. RFID-cards associated to group 8 may change the BDS configuration of section “2”. There are two AC readers with IDs “104” and “105” associated to the BDS – these readers allow normal access control identification when the BDS is disarmed.

Example ReaderProps-table

The ReaderProps table associates digital inputs and relays to the BDS section.

;Ref Reader	Type	Area	Out Arm-Reader	Out Arm-Port	Out Unarm-Reader	Out Unarm-Port	In Rdy-Reader	In Rdy-Port	In Armed-Reader	In Armed-Port	Out-Elapse
0	2	2	999	3	999	4	999	1	999	2	2
;Ref Reader	Type	Area	Code On	Code Off	Group	----	----	----	----	----	---
104	3	2	11	22	8	0	0	0	0	0	0
;Ref Reader	Type	Area	----	----	----	----	----	----	----	----	----
104	4	2	0	0	0	0	0	0	0	0	0
105	4	2	0	0	0	0	0	0	0	0	0

Reader-table

The reader table contains both readers and the controller “999”

ID	ZM	TM	Location	Action	Pin	Ref-Time
104	1	040	1		1004	0
105	1	050	1		1005	0
999	1	320	0		0	0

Action2-Tabelle

The action2 table defines the relays 1 and 2 for opening doors – this is not really necessary for configuring the BDS section.

;ID	RefGroup	RefTime	RefReaderRelais	PortOut	Elapse	RefReaderLED	RefTimeRelais
1004	0	0	999	1	3	0	0
1005	0	0	999	2	3	0	0

Example for the table Identification:

The RFID-Number 59780 can switch the BDS-System and have standard access.

ID	Group	Pin	Duress	ActiveStart	ActiveEnd	ActiveGeneral
51044	1	0	0	2018-01-01	2099-12-31	1
59780	1	0	0	2018-01-01	2099-12-31	1
59780	8	0	0	2018-01-01	2099-12-31	7

5.7.9. Automatic relay release upon opening of the door

Access control:

The amount of time for which a door is being opened is defined by the “Action” table’s “Elapse” property. The door is opened for the amount of time defined by “Elapse” continuously.

With the enhancements of 04.03.13 firmware release, the relay opening the door can now be deactivated (“release”) as soon as a door-open sensor is trigger. This sensor has to present and connected to the access control system mwhen using this function.

5.7.9.1. Supervised doors

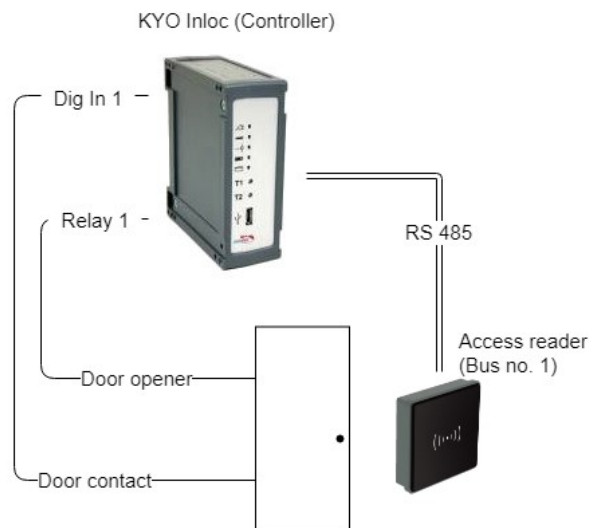


Figure 1 Diagram of a supervised door

A supervised door is a feature of the access controller that allows to lock a door as soon as it has been opened. The supervised door functionality that each door is associated to a digital input that detects if a door is opened. The digital input is assigned using the ReaderProps list.

If the opening of a door is detected, then the associated reader is determined and all realis associated to the reader are deactivated. For this, all actions associated to the reader are checked.



Please Note:

The supervised door functionality will only release relays that have been set for a defined time interval. Doors that are opened by a time model or set to free access will remain opened.



Caution:

All action entries associated to the reader will be checked and released. A check concerning the group is not implemented.

5.7.9.2. Configuration

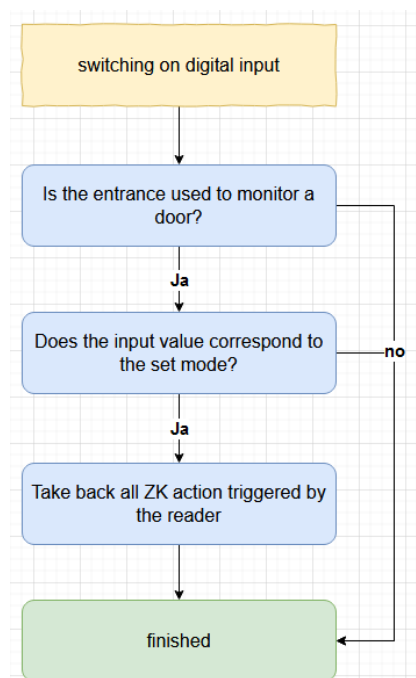
Implementing supervised door using the Datafox Access Control modules requires the setup using the ReaderProps list. This list is required for BDS and anti-passback as well. The following specification of the ReaderProps thus contains minimal field length specifications.

5.7.9.3. Requirements for the ReaderProps entry

The ReaderProps list requires at least 5 columns when used for supervised doors.

Name	Type	Length	Description
RefReader	Number	4	Reference number of the reader, where the relay to be released is placed.
Type	Number	2	Type associated to the supervised door (5) functionality.
Mode	Number	1	Mode used for interpreting the digital input 0 (Input low) = The door is opened 1 (Input high) = The door is opened
RefReaderInput	Number	4	Reference to the reader (or door module or access controller) that provides the digital input for the supervised door.
Input	Number	2	Id of the digital input that changes upon opening of the door. 0 = the door is not supervised. 1-32 = Digital input wired to the door contact

5.7.9.4. Logical conditions implemented by the access controller

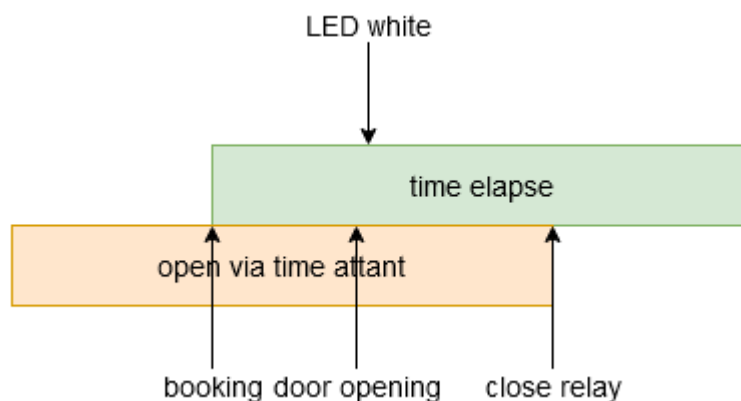


The following conditions are checked by the access controller:


- (1) The check of supervised doors is started upon the change of a digital input.
- (2) Next it is checked, if the digital input (“Input”) and the reader (“RefReaderInput”) are present within the same a supervised door entry of the ReaderProps list.
- (3) If so it is checked, if the input’s state matches the mode (“Mode”). If the Mode is set to 1, the input’s state has to be High (1) has well, for the Mode being 0 the input has to be Low (0). If the Mode matches the input’s state, the state of the relay is checked.
- (4) Next all relays associate to the referenced reader (“RefReader”) that are set for a finite amount of time are being released. If the relay has been set to free access (FRA), blocked access (BLA) or due to a time model associated, it is not released.

5.7.9.5. Special case: Relays operated by time model

Despite a time model being active, the RFID reader will detect and read RFID transponders. The Elapse time associated to the action may overlap with the time model's activity period.



A conflict will occur if the door is opened before the time model expires. In this case the reader's LED is set to white. The relay does not toggle there and switches when the time model expires.

Please Note:  The reader's LED is not set to green if a time model sets the relay. When granting access due to an RFID transponder the LED is set to green only for 3 seconds, not for the elapse time associated to the action. This is the standard behaviour for granting access.

5.7.9.6. Configuration sample

The sample configuration explained here is associated to Figure 1. The digital input 1 is used to detect the opening of the door. A low voltage on the digital input indicated that the door is open.

5.7.9.7. Access control lists

First the two devices are declared by entries to the Reader list. ID 10 is associated to the RFID reader, which is present next to the door. ID 99 identified the access controller.

Reader.txt

ID	ZM	TM	RefLocation	RefAction	PinGeneral
10	1	010	1	100	0
99	1	320	1	0	0

The list Action2 contains the operations for opening the door. Entry 100 will be evaluated when reader ID 10 identified an RFID transponder that is allowed to open the door. The action sets relay 1 at the access controller for 10 seconds. Simultaneously the green LED is activated at reader ID 10.

Action2.txt

ID	Ref Group	Ref Time	Ref Reader Relais	PortOut	Elapse	Ref Reader Led	Ref Time Relais
100	0	1	99	1	10	10	0

The list Time contains time model 1. This time model is active 24/7.

Time.txt

ID	Weekdays	TimeStart	TimeEnde
1	1234567	00:00	23:59

The Location list must contain an entry. This entry associated the time model, so that access using the reader is possible always.

Location.txt

ID	RefGroup	RefTime	RefTimeNoPin
1	0	1	0

In order to open the door, the Identification list must contain an entry that is allowed to open the door.

Identification.txt

ID	Group	Pin	Menace	ActiveStart	ActiveEnd	ActiveGeneral
2059FB3A	0	0	0	2005-04-01	2020-04-01	1

5.7.9.8. Additional lists

As explained earlier, the ReaderProps list is needed in addition to the access control list. If digital input 1 changes to low voltage, all doors being unlocked for a finite time will be locked again. The entry to the ReaderProps list is as follows:

ReaderPorps.txt

RefReader	Type	Mode	RefReaderInput	Input
10	5	0	99	1

5.7.10. Calculation for the power supply of Access modules

When using Datafox access readers or door modules, the necessary cable cross-section has to be calculated before setting up an RS485 network for access control. The voltage drop in the whole bus must not exceed 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	16 V max. 8 V min.DC
TS-TMR33-TM	156,0 mA	16 V max. 8 V min.DC
TS-TMR33-TMR	180,0 mA	16 V max. 8 V min.DC
EVO-reader	250,0 mA	24 V max. 9 V min.DC
PHG-reader	250,0 mA	24 V max. 9 V min.DC

The result is a permissible maximum power consumption per Datafox power supply unit of (8 x 180.0 mA + 8 x 56.5 mA) 1.9 A. 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 setting up and commissioning a ZK-network, the calculation has to be done by a person qualified in this field.

The cable cross-section is calculated as follows:

$$Q = \frac{2 \cdot I \cdot l}{k \cdot U_v}$$

Q = wire size in mm²

I = current

l = wire length in m

k = Conductivity for copper $56 \frac{m}{\Omega \cdot mm^2}$

The following applies for 12 V voltage supply:

U_v = voltage drop. 4V at most. **4 V TMR33**

U_v = voltage drop. 4V at most. **3 V PHG** and Reder **EVO-ZK**

U_v is calculated from the supply voltage minus the minimum voltage for the reader.

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

$$l = \frac{Q \cdot k \cdot U_v}{2 \cdot I}$$

5.7.11. Cable length and cable cross section for access wiring

Wiring:

Cables with a core diameter of 0.6 or 0.8 mm can be used as bus cables.

The following types of lines are suitable, e.g. as bus line:

- J-Y(ST)Y (telecommunication cable),
- YR (jacketed cable),
- A-2Y(L)2Y (telecommunication cable)

Cat 7 Cable for Network structure!

The maximum total line length BUS RS485 A and B wire is 1000 m. Here are one pair for for the A and B data line in use.

Cable lengths for the voltage supply of the readers.

power supply 1 reader from the box to the power supply 12V:

- 0,6 mm Cable cross section: 200 m,
- 0,8 mm Cable cross section: 350 m.

power supply 1 reader with separated power supply 12V:

- 0,6 mm Cable cross section: 250 m,
- 0,8 mm Cable cross section: 400 m.

power supply 2 reader with separated power supply 12V:

- 0,6 mm Cable cross section: 125 m,
- 0,8 mm Cable cross section: 200 m.

power supply 3 reader with separated power supply 12V:

- 0,6 mm Cable cross section: 65 m,
- 0,8 mm Cable cross section: 130 m.

power supply 1 reader with separated power supply 24V:

- 0,6 mm Cable cross section: 500 m,
- 0,8 mm Cable cross section: 800 m.

5.7.12. Status messages of the access control

Display /online	Pre-checked mode for online/offline access	Assigned status message
0		module detected everything OK
3		module not in the list defined but found in the bus rs485
4		module in the list reader added but not found in the bus rs485
5		wrong Encryption password
6		login password is wrong
7		RFID-typ (Mifare, Legic, Unique, etc.) wrong
8		Failed to configure the module
9		No modules
10		the Key for communication with PHG-Modules was changed
11		the Key for communication with PHG-Modules was not changed
12		battery-level of the doorlock phase 0 (full)
13		battery-level of the doorlock phase1
14		battery-level of the doorlock phase 2
15		battery-level of the doorlock phase 3 (empty)
16		Doorlock in mode to change battery
17		Modul Update readdy, important applies to EVO Agera and Interra 2)
18		Reboot after update
19	519	Access denied, because BLA (blocked Access) is activate on this reader
20	520	ID ok, acces succesful
21	521	ID is not in the list identification.
22	522	ActiveGeneral not correct.
23	523	Validity period does not fit.
24	524	Could not find the room. (group definitions)
25	525	Could not find am Time in time-table.
26	526	wait for PIN-input.
27	527	Pin wrong
28	528	threat code was input.
29	529	the PIN is right, acces successful.
30	530	the Master-PIN was input, acces successful.
31	531	PIN-Timeout.
32	532	Master-ID right, acces successful.
33	533	acces successful with PIN input.
34		Online-TP.
35		Online-PIN.
36	536	Make Action closing
37	537	Free access on this reader
38	538	Permanent blocked access
39		Online-result from the server, no access allowed
	256	The server rejects the preliminary test
	257	The server agrees with the preliminary check

Digital	output
40	digital output 1 is low (off)
41	digital output 1 is HIGH.(on)
42	digital output 1 is for the time ELAPSE, HIGH.
43	digital output 2 is low (off)
44	digital output 2 is HIGH.(on)
45	digital output 2 is for the time ELAPSE, HIGH.
46	digital output 3 is low (Off).
47	digital output 3 is HIGH.(On).
48	digital output 3 is for the time ELAPSE, HIGH.
49	digital output 4 is low (Off).
50	digital output 4 is HIGH.(On).
51	digital output 4 is for the time ELAPSE, HIGH.
52 #	digital output 5 is low (Off).
53 #	digital output 5 is HIGH.(On).
54 #	digital output 5 is for the time ELAPSE, HIGH.
55 #	digital output 6 is low (Off).
56 #	digital output 6 is HIGH.(On).
57 #	digital output 6 is for the time ELAPSE, HIGH.

Status messages of the access control

display	Assigned status message digital output
120#	digital output 7 is low (Off).
121#	digital output 7 is HIGH.(On).
122#	digital output 7 is for the time ELAPSE, HIGH.
123#	digital output 8 is low (Off).
124#	digital output 8 is HIGH.(On).
125#	digital output 8 is for the time ELAPSE, HIGH.
126#	digital output 9 is low (Off).
127#	digital output 9 is HIGH.(On).
128#	digital output 9 is for the time ELAPSE, HIGH.
129#	digital output 10 is low (Off).
130#	digital output 10 is HIGH.(On).
131#	digital output 10 is for the time ELAPSE, HIGH.
132#	digital output 11 is low (Off).
133#	digital output 11 is HIGH.(On).
134#	digital output 11 is for the time ELAPSE, HIGH.
135#	digital output 12 is low (Off).
136#	digital output 12 is HIGH.(On).
137#	digital output 12 is for the time ELAPSE, HIGH.
138#	digital output 13 is low (Off).
139#	digital output 13 is HIGH.(On).
140#	digital output 13 is for the time ELAPSE, HIGH.
141#	digital output 14 is low (Off).
142#	digital output 14 is HIGH.(On).
143#	digital output 14 is for the time ELAPSE, HIGH.
144#	digital output 15 is low (Off).
145#	digital output 15 is HIGH.(On).
146#	digital output 15 is for the time ELAPSE, HIGH.
147#	digital output 16 is low (Off).
148#	digital output 16 is HIGH.(On).
149#	digital output 16 is for the time ELAPSE, HIGH.
300#	digital output 17 is low (Off).
301#	digital output 17 is HIGH.(On).
302#	digital output 17 is for the time ELAPSE, HIGH..
303#	digital output 18 is low (Off).
304#	digital output 18 is HIGH.(On).
305#	digital output 18 is for the time ELAPSE, HIGH..
306#	digital output 19 is low (Off).
307#	digital output 19 is HIGH.(On).
308#	digital output 19 is for the time ELAPSE, HIGH..
309#	digital output 20 is low (Off).
310#	digital output 20 is HIGH.(On).
311#	digital output 20 is for the time ELAPSE, HIGH..
312#	digital output 21 is low (Off).
313#	digital output 21 is HIGH.(On).
314#	digital output 21 is for the time ELAPSE, HIGH..
315#	digital output 22 is low (Off).
316#	digital output 22 is HIGH.(On).
317#	digital output 22 is for the time ELAPSE, HIGH..

digital	input
160#	digital input 7 is Low
161#	digital input 7 is HIGH
162#	digital input 8 is Low
163#	digital input 8 is HIGH
164#	digital input 9 is Low
165#	digital input 9 is HIGH
166#	digital input 10 is Low
167#	digital input 10 is HIGH
168#	digital input 11 is Low
169#	digital input 11 is HIGH
170#	digital input 12 isLow
171#	digital input 12 is HIGH
_____	_____continuously until:
210#	digital input 32 is Low
211#	digital input 32 is HIGH

for new devices hardware version 4

BSD/ EMA	Discription/ Beschreibung
258 ¹	The access control system awaits legitimation through RFID transponder and/or PIN after starting a BDS control event due to entering the operating code.
259	The access control system awaits legitimation through RFID transponder and/or PIN after starting a BDS control event due to entering the operating code.
260	During a BDS control event a non-privileged RFID transponder has been presented to the reader. This transponder is either not contained within the Identification table or does not have ActiveGeneral set to 7. See Privileging transponders to control the BDS.
261	The specified BDS section is not configured correctly.
262	There are no concurrent BDS control events supported while a BDS control event is currently being processed.
263 ¹	The BDS signals that is ready to be armed.
264 ¹	The BDS signals that is not ready to be armed.
265	The relay to arm the BDS section has been set.
266	The relay to disarm the BDS section has been set.
267	The BDS section to be armed is already armed. The reader signals "green" anyway so that the operator knows that the BDS section is armed.
268	The BDS section to be disarmed is already disarmed. The reader signals "green" anyway so that the operator knows that the BDS section is disarmed.
269 ¹	The BDS section is armed now.
270 ¹	The BDS section is disarmed now.
271	The BDS section could not be armed within five seconds. The digital input pin associated to the BDS section state still reports the section as disarmed.
272	The BDS section could not be disarmed within five seconds. The digital input pin associated to the BDS section state still reports the section as armed.
273	The access request was denied due to the BDS section being armed.
274	Identification requires an additional PIN.
275	The PIN entered does not match the stored one.
276	The PIN entered matches the stored one.
277	Timeout while waiting for the PIN to be entered.

1) This status code contains the BDS section [1..5] as property „ID number“.

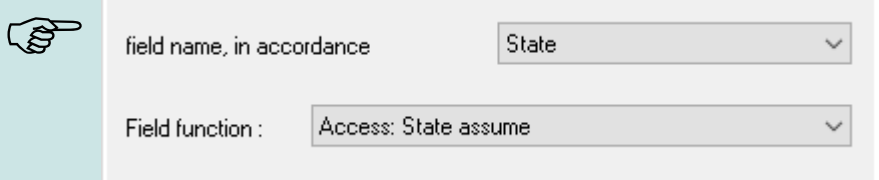
Status messages of the access control

display	Assigned status message		
100	the access-control is off.		
101	server not online (online accses-control)		
102	the device have no lists.		
103	Type not correct in setup settings (GIS, PHG).		
display	Assigned status message		
	Master (ZK-Box / ZK Master)	GIS / TS-Series reader	PHG / EVO-ZK-reader
60	Digital input 1 Master Low	Digital input 1 Reader Low	Digital input 1 (IO-Box is closed)
61	Digital input 1 Master High	Digital input 1 Reader High	Digital input 1 (IO-Box is open)
62	Digital input 2 Master Low	Digital input 2 Reader Low	Digital input 2 (IO-Box closed)
63	Digital input 2 Master High	Digital input 2 Reader High	Digital input 2 (IO-Box open)
64	Digital input 3 Master Low	Digital input 3 Reader Low	Digital input 3 low
65	Digital input 3 Master High	Digital input3 Reader High	Digital input 3 high
66	Digital input 4 Master Low	Digital input 3 wurde unterbrochen	PHG not used
67	Digital input 4 Master High	Digital input 3 wurde kurz geschlossen	PHG not used
68	Digital input 5 Master Low	not used	not used
69	Digital input 5 Master High	not used	not used
70	Digital input 6 Master Low	not used	digital input 1 the Reader Low nicht bei der Voxio-E-Serie
71	Digital input 6 Master High	not used	didigital input 1 on the Reader High nicht bei der Voxio-E-Serie
72		not used	digital input 2 on the Reader Low nicht bei der Voxio-E-Serie
73		not used	digital input 2 am Reader High nicht bei der Voxio-E-Serie
74		not used	tamper switch → OK
75		not used	tamper switch → device manipuliert
display	Assigned status message		
80	alarm-input 1		
81	alarm-input 2		
82	alarm-input 3		
83	alarm-input 4		
84	alarm-input 1		
85	alarm-input 6		
220#	alarm-input 7		
221#	alarm-input 8		
_____	_____ continuously until:		
245#	alarm-input 32		

for new devices hardware version 4

Status message of the access control in a record:

Note:
Do you want see the status from access control, to choose this settings in the Setup.



5.7.13. State signals of reader modules via LEDs

Gelb	Grün	Rot	Zustand des TS TMR33-xx
off	off	off	No supply voltage is present
on	off	off	A supply voltage is present,
on	on (ca. 1 s)	on (ca. 1 s)	Reader recognized and configured by master
on	off	on (ca. 10 s)	Status after module test = status "OK"
on	off	on (permanent)	Acoustic signal by buzzer (approx. 1s) signals module test
flash	off	off	The lists of the access master are updated
on	on (ca. 1 s)	off	Configuration error via the access lists (Checking of the
on	on	on 3 x short	status messages necessary.)
on	flash	off	Signals readable card in the area,

5.7.14. Online functions for the access control

The access control mechanism offers the functionality to control every configuration and action in your software-solution.

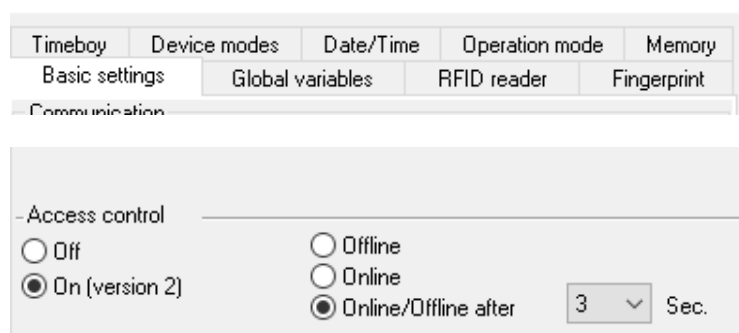
So you can

This allows you to react to all requests from the access control in real time.

Activate the online function in the setup under the basic settings tab.

There are 2 options:

- Offline Mode (the device always waits for the answer from the server)
- In the option **Online/Offline** the terminal waits a defined time before switching to the offline functionality. If this happens the terminal will use the access lists in its memory.



5.7.14.1. Online via http-protocol

The communication with http is very quick and easy to set up. Therefore the webserver has an easy job to react to the requests in a very short period of time.

Requirements:

Hardware:

- TCP/IP
- GPRS (1-2 seconds delay)

Software:

- Active Script with a logic for the access control and specially designed to suit the connected hardware (access reader)

With the answer from the server you are able to perform specific actions with the access readers.

The following examples will give you an insight in what is possible with the functions and actions. All parameters correspond the online functions with the dll.

Example 1:

The following data is going to be received

`table=access&date_time=2013-07-05_07%3A48%3A11&Master_ID=1&Modul_ID=010&Chip_Nr=2058&Status=34&checksum=2461`

<code>Master_ID=1</code>	Master-ID
<code>Modul_ID=010</code>	bus adress of the reader / TM
<code>Ausweis_Nr=2058</code>	ID of the read Chip
<code>Status=34</code>	Online (34)

Fitting answer to grant access:

`status=ok&checksum=2461&access=010&mask=8&type=1&duration=1`

With firmware-version 04.03.04 and up also possible is:

`status=ok&checksum=2461&master=1&module=010&mask=8&type=1&duration=1`

<code>access=010</code>	bus adress, on which the action will take place (FW 04.03.03 and lower)
<code>module=010</code>	bus adress on which the action action will take place
<code>master=1</code>	rs485-bus on which the action action will take place
<code>mask=8</code>	relais Nr.1
<code>type=1</code>	turn-on
<code>duration=1</code>	for 1 second

Fitting anser to deny the access => Red-LED:

`status=ok&checksum=2482&access=010&mask=5&type=1&duration=2`

ab der Firmware 04.03.04 ebenfalls möglich ist:

`status=ok&checksum=2461&master=1&module=010&mask=8&type=1&duration=1`

<code>access=010</code>	bus adress, on which the action will take place (FW 04.03.03 and lower)
<code>module=010</code>	bus adress on which the action action will take place
<code>master=1</code>	rs485-bus on which the action action will take place
<code>mask=5</code>	red LED + buzzer
<code>type=1</code>	turn-on
<code>duration=2</code>	for 1 second

Several bus strings can be controlled with the new hardware V4. In order to be able to execute actions on the corresponding bus string, the bus string ID must be transferred with the response as well.

For this, the new keywords "module" and "master" were implemented. These must be used together, replacing the keyword "access".



Attention:

The order "**access→mask→typ→duration**" or **master→module→mask→typ→duration** must be strictly adhered to.

`status=ok&checksum=2482&access=010&mask=5&type=1&duration=2`
`status=ok&checksum=2482&master=1&module=010&mask=5&type=1&duration=2`

Overview of the possible parameters for the keywords:

keyword	value / Bit Nr.	description
access= or module= function for 1x Bus RS485	000 010 011 ... 081 usw.	The value of the string must follow the format of the "TM" field of the "Reader" list. He must therefore always include 3 digits.
master =	1-3 1 2	Id for the RS485 bus ZK, represents the ZK- rs485-bus. RS485 Bus ID 1 RS485 Bus ID 2... „ master “ has to be set together with „ module “ and so replaces the function „ access “
mask	1 / 0	this bit will trigger the buzzer.
	2 / 1	this bit will trigger the green LED.
	4 / 2	this bit will trigger the red LED.
	8 / 3	this bit will trigger the first relay.
	16 / 4	this bit will trigger the second relay.
	32 / 5	this bit will trigger the third relay.
	64 / 6	this bit will trigger the fourth relay.
	128 / 7	this bit will trigger the fifth relay.
	256 / 8	this bit will trigger the sixth relay.
	unused. always set to 0
type	0	Off
	1	On
	2	change (600ms on, 600ms off)
	3	3 times on for 500ms
duration	Sekunden / 0	Is a period of time and only at =1 active. meaning: 0 = always on, 1 - 40 = seconds on.



Hint:

You can also perform multiple actions on the access control in one response. However, the total length of the response must not **exceed 254 characters**.

Attention:

A automated switch between online and offline mode is not possible in http mode



- Access control

Off
 Offline

On (version 2)
 Online

Online/Offline after
 Sec.

5.7.14.2. Online via DLL connection

The dll offers the function to directly access the external access reader. With the function “DFCEntrance2OnlineAction“you are able to trigger the buzzer, the LEDs and the relays.

In the case of an access booking, the access master generates a data record. This must be picked up immediately and forwarded to the application on the server. The application then decides whether access is granted and returns a command to control the relay in the door module or lets the buzzer sound and issues a visual message via the LEDs.

More dll functions are documented in the “Datafox SDK” on our website

https://www.datafox.de/downloads-datafox-kyo-inloc.de.html?file=files/Datafox_Devices/Downloads_Geraete_Zubehoer/001_MasterIV-Software/Datafox_SDK_Windows_04.03.12.zip

5.7.15. Function for access control U&Z (locking cylinders)

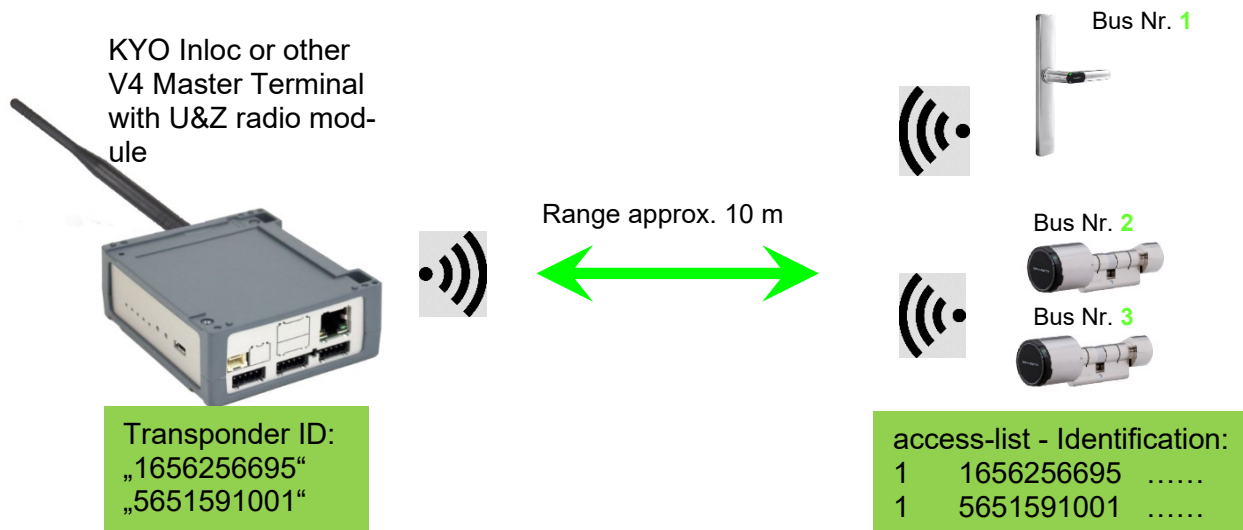
5.7.15.1. Design example

The radio locking cylinders are set up and integrated via the standard Datafox access control system. The PHG crypt protocol is used. All data is thus securely encrypted.

Functionality:

The electronic locking systems read an RFID chip / card and transmit the read information to Datafox access control. The Datafox access control then decides on the basis of the access logic whether the door is opened or not.

Design example with integrated radio module in the KYO Inloc.



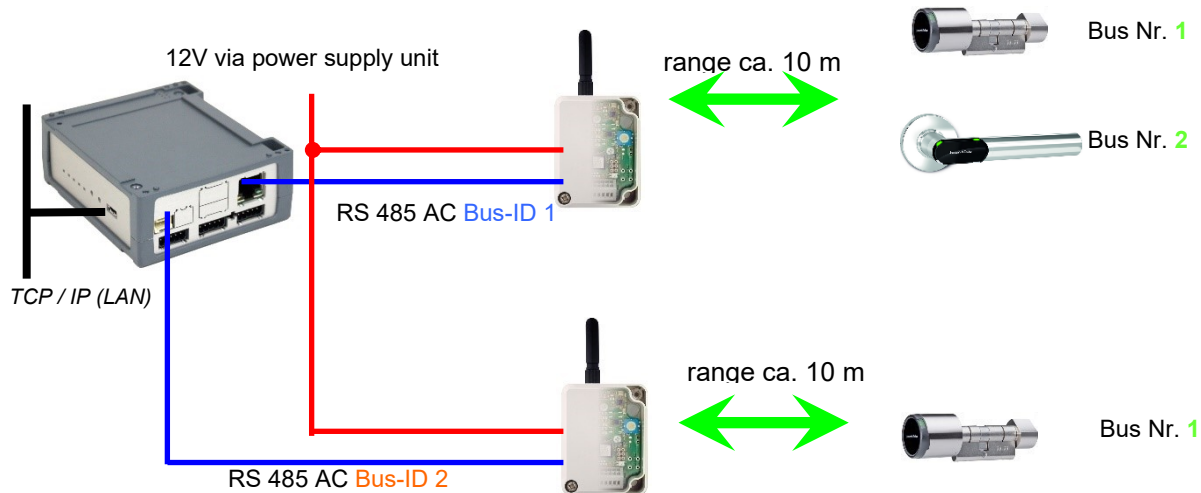
Entsprechende Reader Tabelle, Beispiel:

ID	ZM / Bus-ID	TM (Busadresse)	RefLocation	RefAction	PinGeneral	Description-text
1	1	010	1	1	0	Reader - RS485 module slot 1 = Bus ID 1
2	1	020	2	2	0	Reader - RS485 module slot 3 = Bus ID 1
3	1	030	3	3	0	Reader - RS485 module slot 7 = Bus ID 2

Note: The transponders are read by the cylinder and the ID is transferred to the ZK-Box. It then decides whether the ID access is granted and sends a corresponding signal to the cylinder.

Note: Only one radio lock cylinder can be used at a time!
From booking to termination of the radio connection we need approx. 2 seconds for a rejection. With an opening approx. 1 second.
If ID cards are held on two or more doors at exactly the same time, the first locking cylinder has the connection with the FSM for approx. 2 seconds. If a radio lock cylinder does not receive a radio connection after 1 second, it performs an offline check. If no ID cards have been deposited, they will no longer respond to the ID card. The badge is then stored in the reader and the system no longer reacts to this badge (repeat posting block) until another badge is available.

Construction example KYO Inloc with two external radio- or BLE- modules.

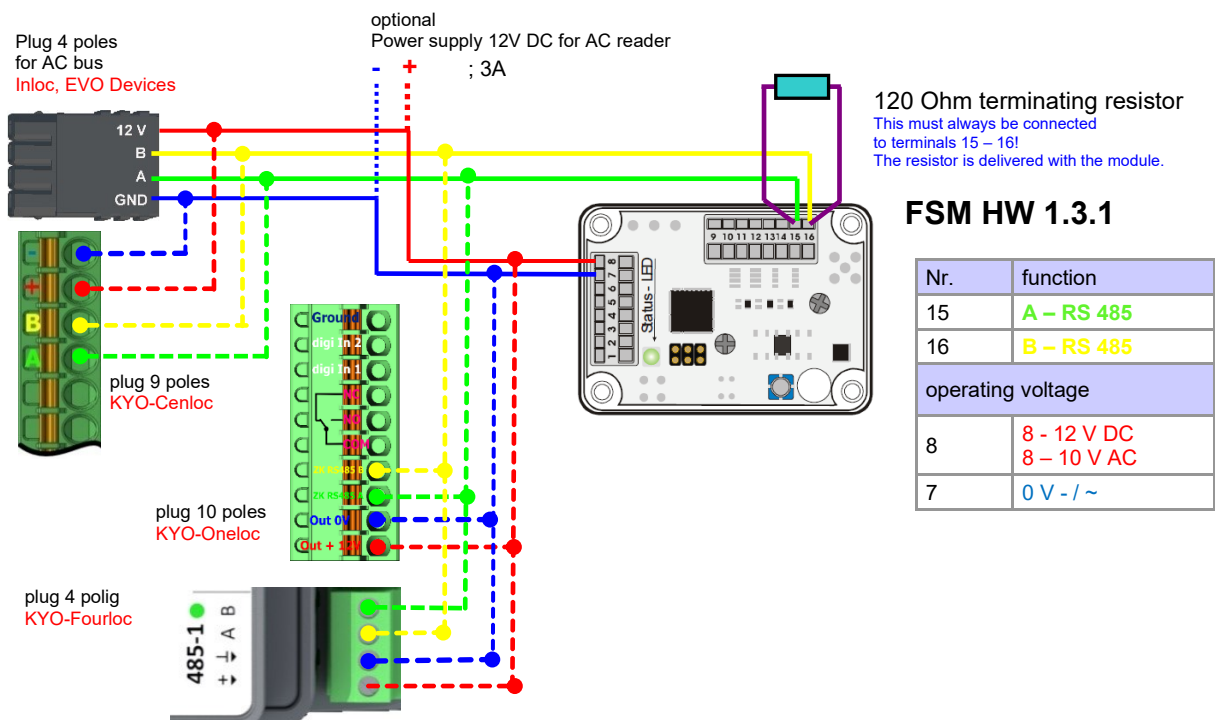


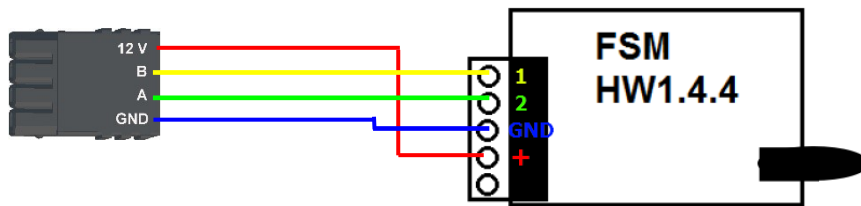
Corresponding reader table, example:

ID	ZM / Bus-ID	TM (Bus-address)	RefLocation	RefAction	PinGeneral	Description-text
1	1	010	1	1	0	reader RS485 module slot 1 = Bus ID 1
2	1	020	2	2	0	Reader RS485 module slot 3 = Bus ID 1
3	2	010	3	3	0	reader RS485 module slot 7 = Bus ID 2
4	1	320	0	1	0	KYO Inloc (Master-device)

Wiring diagram of the different bus connections with external radio module:

(In this case, the same structure applies per access control string or ZM / Bus-ID)

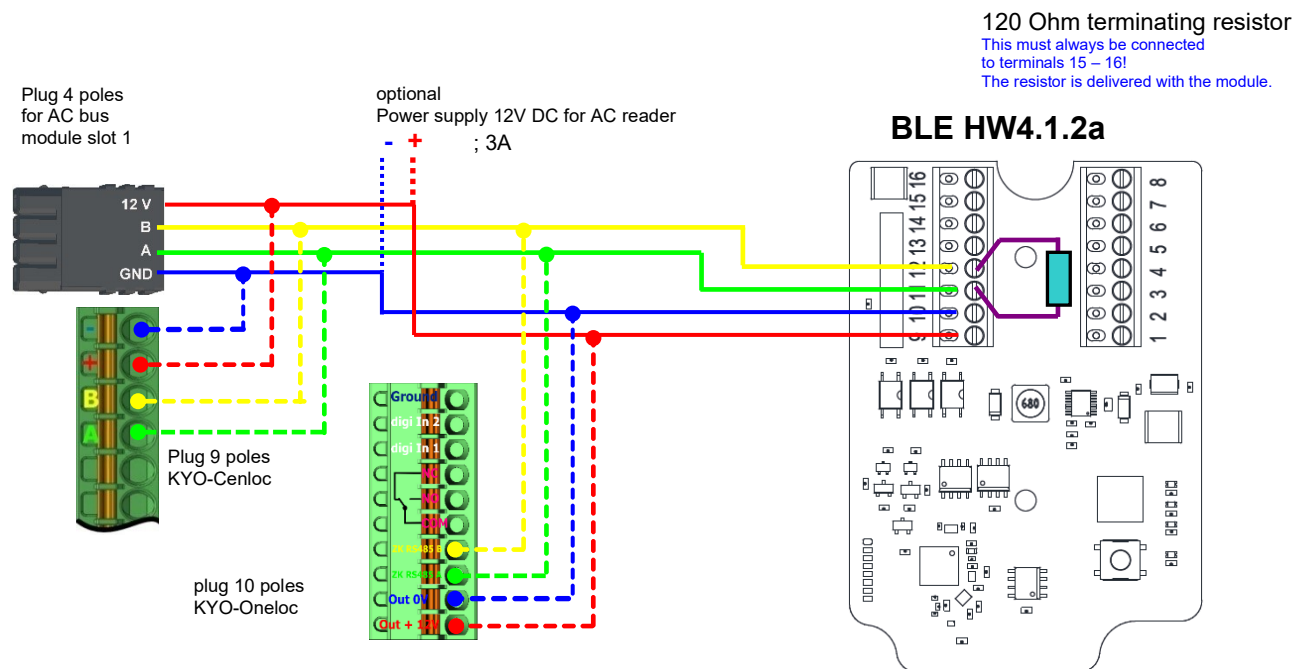




Nr.	function
1	B – RS 485
2	A – RS 485
Operation voltage	
GND	0 V +/- ~
VCC	8 - 12 V DC 8 – 10 V AC

Wiring diagram of the different bus connections with external BLE-Modul:

In this case, the same structure applies per access control string or ZM / Bus-ID



120 Ohm terminating resistor
This must always be connected to terminals 15 – 16!
The resistor is delivered with the module.

BLE HW4.1.2a

Nr.	function
11	RS 485 - A
12	RS 485 - B
Operation voltage	
GND	0 V
VCC	5 - 24 V DC

5.7.15.2. First start with locking cylinders

The scope of delivery always includes a service card.
To install the cylinders, you also need a disassembly card.
These have not yet been created in their as-delivered state.

Hold the service key in front of the knob module. (A)
An optical/acoustic signal indicates that the programming mode is active (possibly before this step, the wake-up function of the knob module may be required by turning it)



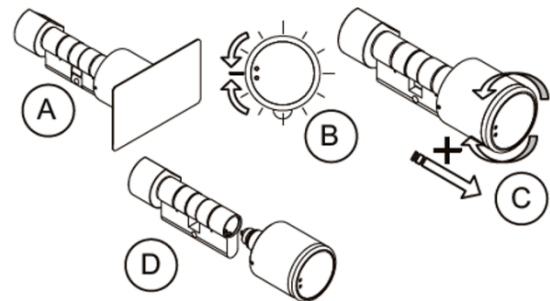
With firmware 2.7.0, there is only an acoustic signal about activation of the service mode!

Teaching:

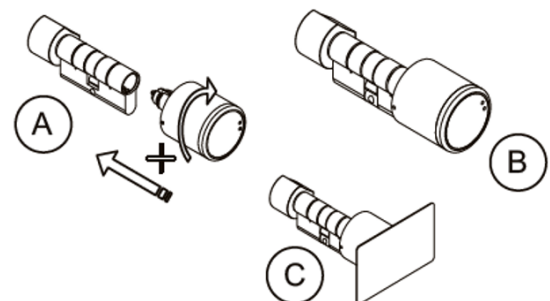
- 1) The first card that is held = **battery exchange card**
- 2) The second card becomes the = **disassembly card**

5.7.15.3. Assembly and disassembly of the cylinders

- 1) Hold the disassembly card in front of the knob module (A)
(Possibly the knob module may need to be woken up by turning the knob before this step).
- 2) Knob module enters disassembly mode.
- 3) Turn the knob module until the emergency power contacts are in the 9 o' clock position. (B)
- 4) Remove the knob by slightly turning it back and forth and pulling it lightly at the same time. (C+D)



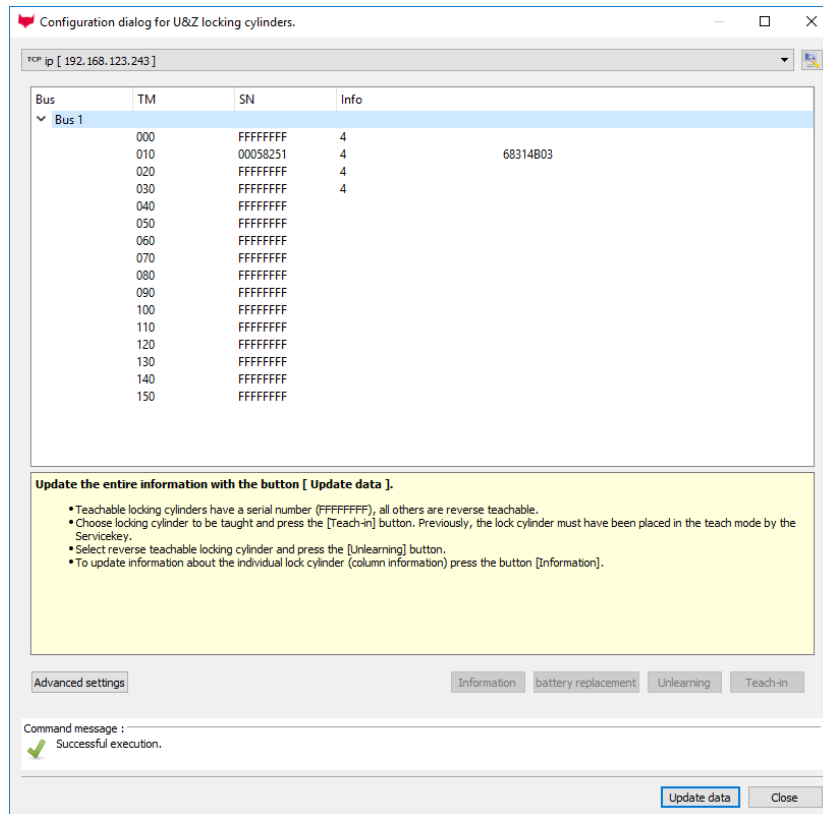
- 1) Carry out steps 1 and 2 as described in the point above (not necessary if the knob module is still in disassembly mode).
- 2) The knob module is mounted in the cylinder housing by inserting and simultaneously rotating it. (A+B)
- 3) To reset the disassembly mode, hold the disassembly card or an authorized transponder in front of the knob module. (C)



5.7.15.4. Set up the wireless network for cylinder

For setup, DatafoxStudioIV can be used in conjunction with the service key card. To do this, select "Configuration→Access control→Configure U&Z locking cylinder" in DatafoxStudioIV. With "Update data" the current configuration is read from the FSM.

In connection with the BLE module, only addresses 000 - 070 can be used.



Steps of teaching-in the cylinders:

1. Hold service key to cylinder

(Service = 20 seconds active (activate cylinder by turning it briefly!))

2. Refresh data in DatafoxStudioIV!

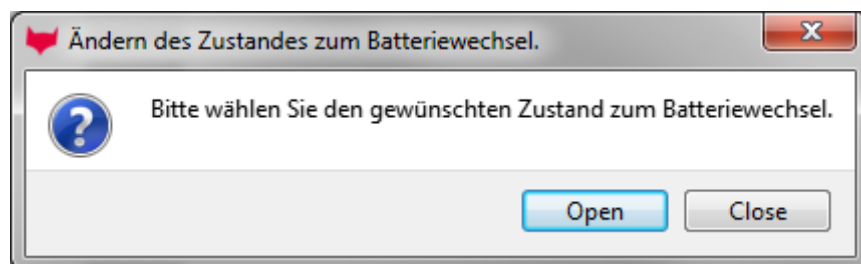
Free addresses are displayed with FFFFFFFFFF, the serial number of the radio lock cylinder and the status of the modules are displayed for the assigned addresses, as in the dialogue Status of the access modules.

The "Configuration dialog for U&Z locking cylinders" dialog allows different things to be done.

Advanced settings:

- Setting the ZK-Master ID for the device
- KnobActiveTime: Time that the cylinder tries to reach the FSM after activation until it goes back to standby.
- Update information on individual locking cylinders (column "Info")
- Changing the battery puts the radio lock cylinder into a mode that allows the cover to be removed and the battery to be changed. To do this, brief communication with the FSM is required. This is achieved by turning the knob or holding a transponder in front of it.
- Teach out: The cylinder is removed from the FSM and can be taught in to another FSM.
- Teach-in: To connect a radio lock cylinder to the FSM (the radio lock cylinder then only communicates with this FSM)

5.7.15.5. Battery state and live time



With "Open" the command to open is sent to the FSM. This stops the command until a radio connection is established. This can be achieved by turning or holding a transponder in front of it. The locking pins of the hood are then unlocked.

With "Close" the command for locking the hood bolts is sent back to the FSM. However, the lock is only established after a good entry / opening.

The three phases of battery management

Phase 1

If an authorized ID card is held in front of the knob module, the locking authorisation is granted in accordance with the programming. However, the door opening is accompanied by 5x red flashing (LED) and 5 short acoustic signals at the same time.

Phase 2

If an authorized ID card is held in front of the knob module, the locking authorisation is only granted after approx. 5 seconds according to the programming. During these 5 seconds the LED flashes green. The door opening is accompanied by 5x red flashing (LED) and 5 short acoustic signals.

Phase 3

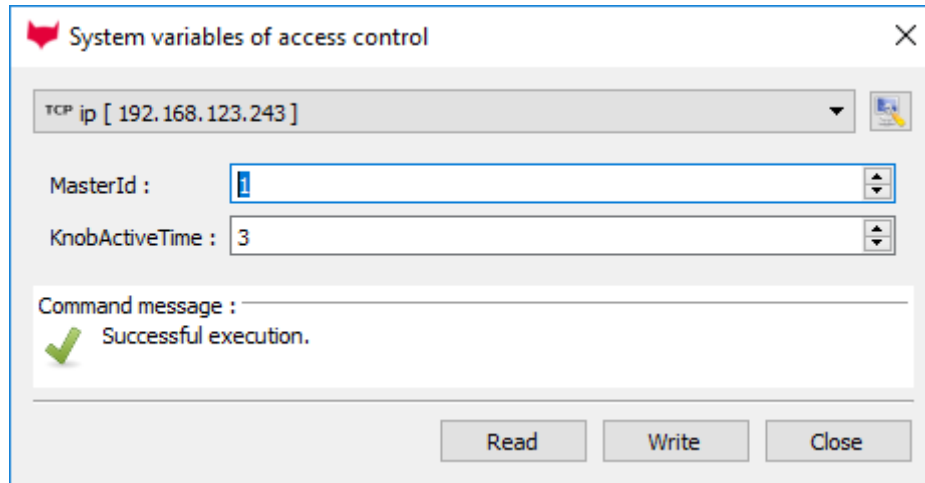
The knob module no longer responds to authorized ID cards. Replace the battery immediately. This is now only possible using the service key and the service device or the battery replacement card.

Please also note the corresponding status messages from the access control system:

display	Assigned status message
0	Module detected, everything's OK.
12	Battery status of the radio lock cylinders in phase 0 (full)
13	Battery status of the radio lock cylinders in phase 1
14	Battery status of the radio lock cylinders in phase 2
15	Battery status of the radio lock cylinders in phase 3 (empty)
16	Radio lock cylinder set to battery change mode

5.7.15.6. Change the access control master ID and knob Active Time

To change the access control master ID, the "Configuration dialog for U&Z locking cylinders" dialog must be used. It contains "Advanced settings" and with a click on it this dialog opens.















Master ID can be set in the range from 1 to 9999. If a device has more than one access control bus, the access control master ID is the ID of the first bus. The second bus access-control-Master ID + 1 etc.

The Knob Active Time is for presetting how long a radio lock cylinder maintains radio communication with the FSM when activated. When a transponder booking is made, the access control master automatically closes the connection after signaling and opening. If the Knob Active Time is less than required for the transponder booking, the radio lock cylinder switches off and an opening fails. This happens at e. g. Knob Active Time = 1 (1s). If someone turns the knob of the radio lock cylinder, the radio connection to the FSM is established and the connection remains active as long as the Knob Active Time is active. Useful values are between 2 and 10 seconds. By default, this time is set to 3 seconds.

It makes sense to increase the value if three or more radio participants are connected to a radio module. Recommendation: KnobActiveTime = 6 seconds

5.7.15.7. Optical and acoustic signals of the U&Z locking cylinder

function	sounds	Optical signals
sleep mode		
Start programming mode	- O	 (except with FW 2.7.0)
badge trained	O O	
Badge deleted	- -	
warning signal Delete all badges	O O O O O 15 sek.	
End of programming mode	O -	
After wake-up - Read mode		
Badge not authorized	- - -	
badge authorized	O	
After battery change	- - -	 
No radio link (out of range)	No sound	 long  short  short

 = red lights up

 = red flashing

 = green lights up

 = green flashing

- = long low tone

O = short beep

5.7.15.8. Optical and acoustic signals of the U&Z door handle

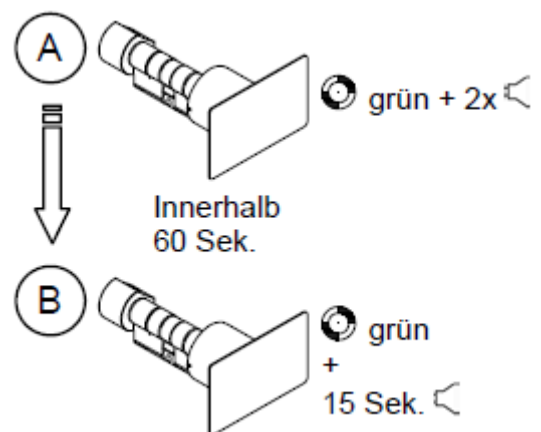
function	sounds	Optical signals
Sleep mode		
Begin programming mode	- O	
End programming mode	O -	
Badge trained	O O	●
Badge deleted	- -	●
After wake-up - read mode		●
Badge not authorized	- - -	●
Badge authorized	O	●
Reset	-	● ●
Battery warning Phase1	O O O O O	● ● ● ● ●
Battery warning Phase2	O O O O O	● ● ● ● ● ●

● = red lights up ● = red flashing
 ● = green lights up ● = green flashing

- = long low tone
 O = short beep

5.7.15.9. Resetting the U&Z locking cylinder

- 1.) The knob module must have been taught out in the radio module.
- 2.) Hold the service key in front of the knob module for the duration of a programming mode (15 seconds) and repeat the procedure within 60 seconds. At the end of the second programming mode, this deletes all badges (incl. battery change and disassembly card) except for the Servicekey. (A+B)
- 3.) The existing badges can then be re-learned as described in section 9.1.
Here, the first ID card held is used for the battery change card and the second to the disassembly card.



5.7.15.10. Supported transponder technologies

Transponder for 125kHz

Supported is

- read Unique
- read Hitag1
- read Hitag2 **only serial number**

Not supported is

- reading of Hitag2 segments
- reading of Titan, Q5 und ATA5577

Mifare Classic

Supported is

- read UID
- read Sector/Block

Not supported is

- Autologin (for reading all passwords)

Mifare Plus

Supported is only Security Level 1

- read UID
- read Sektor/Block

Not supported is

- Autologin (Use the default passwords for reading)
- Random UID (Read true UID at Random UID badges)

Mifare Desfire

Supported is

- read UID
- Read file (max. 220Byte)

Not supported is

- Random UID (Read true UID at Random UID badges)

Legic Prime and Legic Advant

currently no restrictions are known.

1.1.1.2 Service key broken / lost

In the case that an authorization medium is damaged or lost, a replacement service key (CX2352) can be ordered from U&Z with the system card.

The system card must therefore be kept safe and inaccessible to unauthorised persons.

1.1.1.3 Replace service key

The service key can be replaced by another one.

Method:

1. Hold the current service key in front of the knob module until the programming mode is active.
2. Hold the new service key in front of the knob module until an optical/acoustic signal indicates that the service key is taught in.

1.1.1.4 Technical data of the radio module

Technical data CX 6932	
<p>dimensions radio module without antenna: 65x50x40 mm radio module with antenna: 111x50x40 mm</p>	<p>Environmental conditions Operating temperature: -20°C to 65°C Storage temperature: -40°C to 85°C Installation location: Indoor and outdoor areas (depending on the product design). Avoid shading! When used outdoors, the external conditions must be checked.</p>
<p>Power supply Supply voltage: 8-20V= or 8-16 V~ Power consumption: Typ. 10mA (standby), max. 50mA (send/receive)</p>	

5.7.16. Office mode using Uhlmann&Zacher radio locks

This chapter describes how an office mode access can be configured using U&Z radio locks or door fitting. This chapter will address both options as “U&Z radio locks”.

5.7.17. Office mode implementation (Variant 1 – Secure Method)

When configuring the access control system, each RFID tag will be associated to an opening period. The opening period can either be set through the elapse property inside the Action2 table or be derived from a time model. If the resulting opening period is longer than 3 seconds, the RFID-card is considered to be office mode enabled – a typical door opening period is 3 seconds.¹

5.7.17.1. Activating office mode

If an RFID-card is presented to a U&Z radio lock, the lock creates a radio connection to the access controller in charge. Should the access controller determine, that the door is not in office mode and

- the transponder is not “office mode”-enabled, it will process the RFID-card using the normal access control logics. When being done, the result is sent to the U&Z radio lock, which then will perform proper signalling and open the door – if permitted.
- the RFID-card is office mode enabled, the door will be set to office mode until the end of the opening period. The information of granted access will be sent to the U&Z radio lock, which will signal green (and open the door).

5.7.17.2. Operation in office mode

If a door is in office mode, the door can be opened with or without presenting an RFID-card to the U&Z radio lock. The lock will receive the access grant from the access controller directly when the U&Z radio lock is being operated as wakes up.

Should an RFID transponder be presented to the U&Z radio lock that is in office mode, its transponder access permissions will be evaluated resulting in red (no access) or green+red² (access) signalling – depending on the access permissions of the transponder. The door – being in office mode – will open independently of the signalling here – so an RFID-card may be checked for access permission even in office mode.

After having opened – not depending on office mode or normal access grant from an RFID-card – the door will be accessible for roughly 5 seconds. After that period the U&Z radio lock will autonomously decouple, so that the door is not accessible any more.

If a U&Z radio lock is operated, it creates a radio connection with the access controller. If the office mode for this radio lock is

- active, the access controller instructs the radio lock to couple, so that the door can be opened
- inactive, a normal transponder based access control is performed.

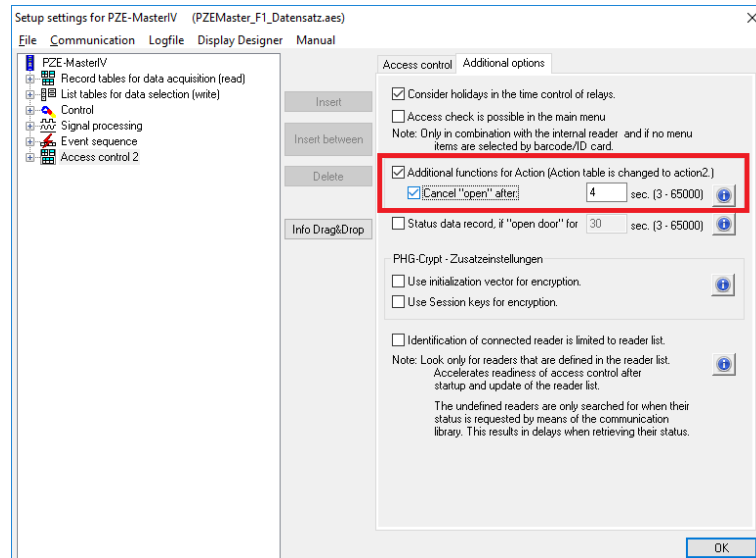
Please note: Please keep in mind, that setting up the radio communication and checking, if the door is currently in office mode, can require 1 to 2 seconds. During this time the U&Z radio lock will not open – this will be possible after having checked the office mode with the access controller. The completion of this check is indicated by flashing of the green LED.

¹ If you configure a time model a an elapse time, then the door is opened during the time model for the elapse time. Should the time model be from 08:30 to 16:00 o' clock with an elapse time von one hour, there may be a permanent opening until 16:59. It is not removed at 16:00.

² We are aware that some U&Z radio locks come with a multi-colour LED. For these red and green light will mix to yellow light.

5.7.17.3. Revoking office mode

If you want to be able to revoke office mode before the opening period is exceeded, you can activate the option “Cancel open after”. If you present an office mode enabled RFID-card to the U&Z radio lock within the configured period (4 seconds according to screenshot below), the office mode will be revoked from the door.



Presenting the transponder for the first time during office mode will result in green and red LED being activate simultaneously. The U&Z radio lock will then beep once – now the period for cancelling the office mode is active. If the same transponder is presented a second time within the cancellation period, the office mode is revoked for the lock which is signalled by a short beep and the green LED.

5.7.17.4. Summary

Using this approach we can provide office mode behaviour using U&Z radio locks. The solution implemented

- is optimal concerning the energy consumption if the U&Z radio lock (there is no continuous radio connection between the radio lock and access controller)
- safe in the case of power outage, since the doors will be locked automatically then.

5.7.18. Office mode implementation (Variant 2 – Classic Method)

In classic mode, the a door’s radio lock locks in permanently, so that the radio lock may be operated as if it were a classic door control.


5.7.18.1. Office mode in classic mode

In classic mode the permission to put a door into office mode (and revoke it from the door) is tied to an ID card. After the office mode is activated, the radio lock will couple – the door can then be opened immediately. The radio lock does not have to ask the access controller to permit opening the door.

After revoking the office mode the door lock uncouples. After that the door is locked again and may be operated after normal access control identification process.

To activate the classic mode, an ID card with specific permission has to be presented to the same door lock twice within 15 seconds (hereafter: office mode repetition interval, short OMRI). The same sequence is used for deactivating the classic office mode.

Both identifications for either activating or deactivating the classic mode have to be done using the same ID card. The OMRI is not configurable.

Attention:  We consider this office mode variant to be unsafe compared to the secure variant mentioned above. In case of power outage, malfunction of the access controller or disruption of the radio communication an opened door remains open. Thus we recommend to use the secure method.

5.7.18.2. Configuring classic office mode

To enable classic office mode, the “identification” list has to be modified. ID cards being allow to perform classic office mode operation require the have the „ActiveGeneral“ parameter set to „6“. ID cards of this type are hereafter designated as “permanent-open” ID cards.

Example for an „identification“ list entry:

Id	Group	Pin	Duress	ActiveStart	ActiveEnd	ActiveGeneral
123456	1	0	0	2017-01-01	2018-01-01	6

5.7.18.3. LED and Buzzer feedback in classic office mode

This chapter explains the feedback offered at a radio lock:

No.	State before action	Action	State after action	Green LED	Red LED	Relay
1	Classic mode inactive	Normal, valid access control identification of first identification of a permanent-open ID card.	Classic mode inactive	2x short flashes + 1x beep	-	Is set for X seconds
2		Invalid access control identification		-	3x short flashes + 3x beeps	Not switched
3		Second identification with the same permanent-open ID card outside the OMRI.		see 1		see 1
4		Second identification with a different permanent-open ID card during the OMRI.				
5	Classic mode active	Second identification with the same permanent-open ID card during the OMRI.	Classic mode active	2x short flashes + 2x beep	-	Is set permanently
6		Valid, invalid or first identification of a permanent-open ID card		1x short flash + 1x beep		Stays permanently set
7		Second identification of a permanent-open ID card outside the OMRI.				
8		Second identification of a different permanent-open ID card during the OMRI.				
9		Second identification of the same permanent-open ID card during the OMRI.	Classic mode inactive	-	2x short flashes + 2x beeps	Is set permanently

5.7.19. Operation / activation-deactivation the Office-Mode

5.7.19.1. activation

1 Holding the office mode authorized badge

The LED flashing green

2 Move the door handle / lock and wait 3 seconds for the door to open normally once. Slide the ID card out of the RFID field. (While opening the door handle or the door lock, no further bookings are accepted)

3 again hold ID card within 15 seconds.

The door handle flash green, green with two short beeps.

The office-mode is directly active!

5.7.19.2. deactivation

1 Holding the office mode authorized badge

The LED flashing green

2 Slide the ID card out of the RFID field.

3 again hold ID card within 15 seconds.

The door-handle flashing red, red with two short beeps.

The office-mode is deactivated!

5.7.19.3. Remarks

- A radio lock may only have one office mode assigned: You may either use the secure variant (with a big elapse time) or the classic mode.
- If an ID card is set to “Active General” 6, an elapse time bigger than 3 seconds may be set.
- Revoking classic office mode requires identification with the same ID card twice within the office mode repetition interval:
 - Activating or deactivating the classic office mode requires that – after the first identification – the elapse time has to have passed.
Reason for this is that while the door relay is set (which it is during the elapse time), the communication of the radio door control unit is paused as well as its reading of ID cards.
- If a permanent-open ID card is restricted in time, activating the classic office mode is possible only during the restricted time.
- Deactivating classic office mode is possible at any time using a permant-open ID card – even outside the restricted time of the ID card.
- If classic office mode is active, the door feedback – indepently of the validity of the ID card – is always green – the door is currently opened.
- Due to the radio locks being battery powered, LED feedback is possible only directly after operating the radio lock.
- After activating the classic office mode and a subsequent restart of the access controller, the door may be used once without prior identification. Then the radio lock decouples and the door is locked.
 - Background: The first operation of the radio lock (reading an ID card or operating a door knob) after restarting the access controller will set the radio lock it its default state.
 - After setting the radio lock to its default state it is in state “classic mode inactive” – the LEDs will signal accordingly.

5.8. Data on Card

5.8.1. General infomations

With the Data on Card - function it is possible to write data with an individual structure on a transponder.

These data are provided in the form of a list of your application.

This list is loaded onto the terminal, and if you're holding the transponder in front of the terminal the data will be written and saved.

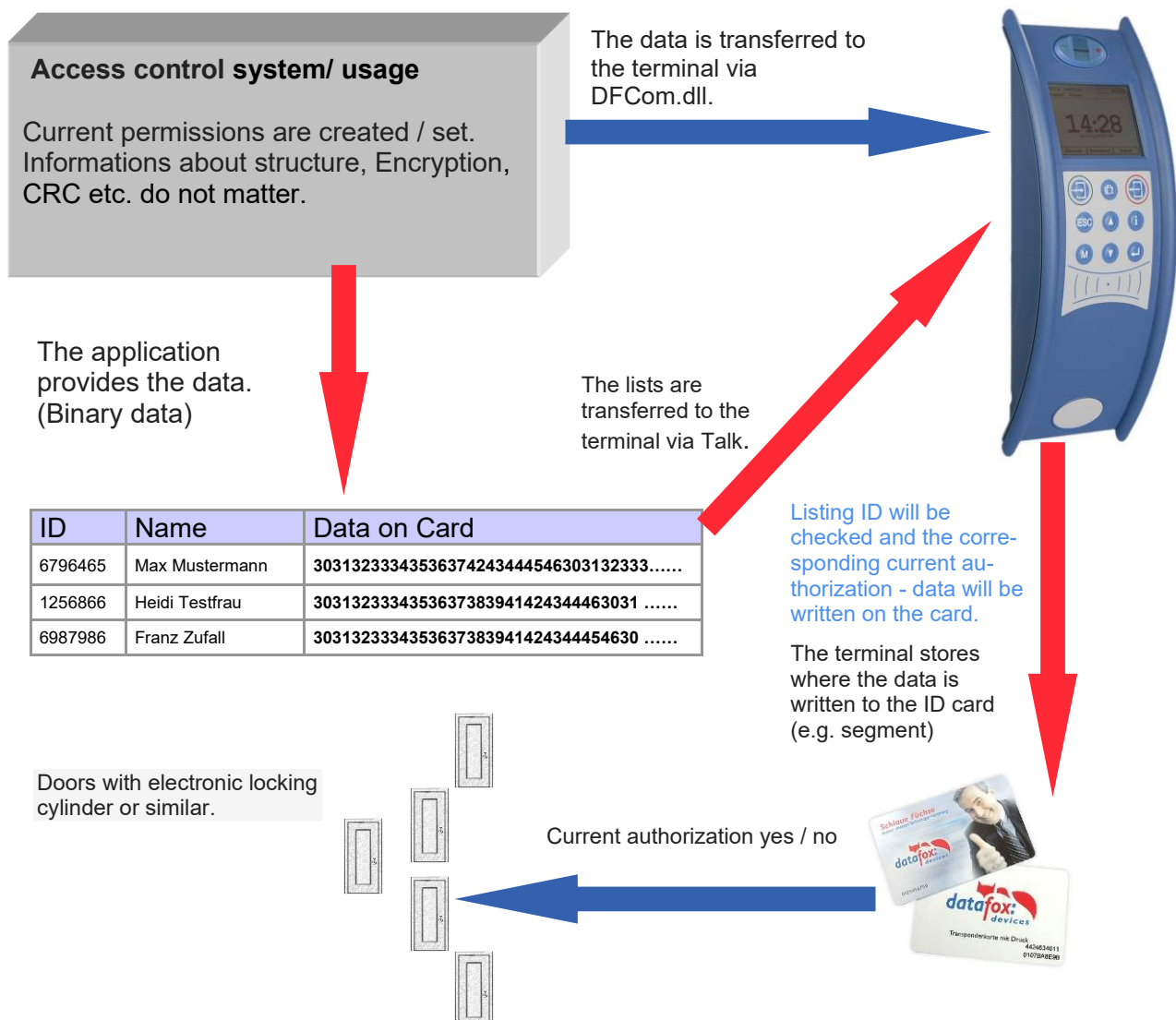
The following transponder-procedures support the Data on Card-function:

- Mifare
- Legic
- iCode
- MyD

For instance:

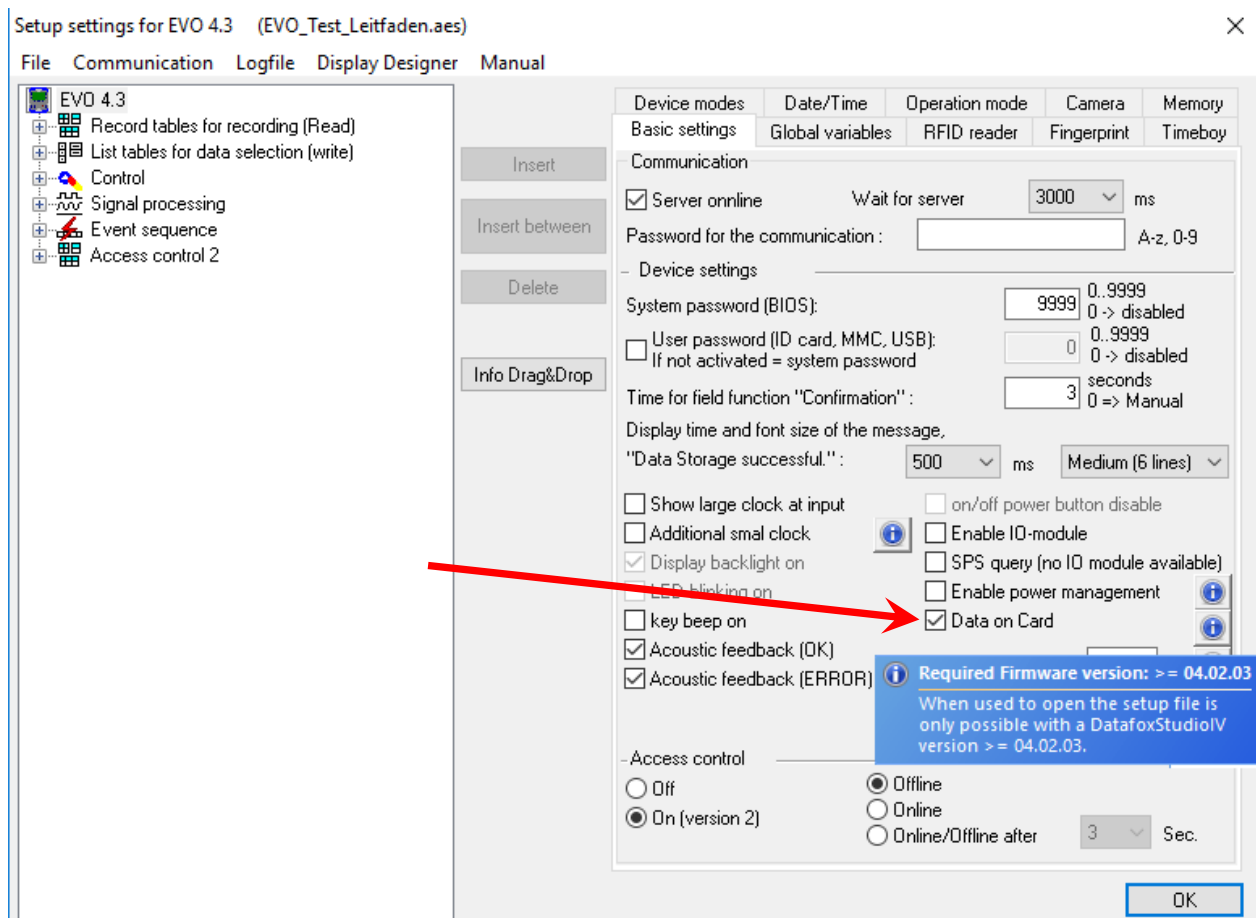
In buildings with an electronic closing cylinder should the actual daily authorization for the access be wrote down on a transponder card.

The Personal ID will be checked and the corresponding current authorization - data will be written on the card. The terminal stores where the data is written to the ID card (e.g. via segment).



5.8.2. Settings for using DataOnCard

Data on Card is an option of the device where data can be written to a transponder from a data list. This option needs to be stated and said while you ordered your product. Those devices who don't offer this option, an error message will be displaying when it's executed.



Data on Card works in 3 steps:

- reading a value from the transponder, e.g. Serial number
- the value is used to select a binary field list to read the binary data
- the binary data is written to the transponder

The return value of the Data on Card function for GV or data record field is the value from the first step "Reading a value from the transponder".

For errors like "the value is not found on the list" or the "writing to the ID failed" the function generates an ESC.

The side steps can then be used to decide how the work continues in the input chain.

The binary field data within the file that the DatafoxStudioIV imports and transmits is to be specified as a hex string. When importing via the DLL, the data needs to be passed on as binary data.

Using the DFC GetField, DFC GetField list functions, you are working with strings, while the firmware converts the hexstrings to and from the binary data.

Settings for Data on Card

Setup settings for EVO 4.3 (EVO_Test_Leitfaden.aes)

File Communication Logfile Display Designer Manual

Data on Card

Selection value read from ID card
RFID reader configuration: **1.)** Default

List with data: **2.)** Personal Data

First Selection field from list "Personal Data": UID

Field with data to be written: Binary

Behavior when there is no entry for the selection.
 Output error message (generated ESC, see jumps)
 No error message output (generated ENTER)
 Branch to: Parent submenu

3.) Write ID card value
 RFID reader configuration: Config. 1
 Big Clock hide and show message for writing.

Behavior at the end of the function
 Return to the confirmation required
 or automatically hide after 0 seconds.

OK

1.) RFID Configurations for the RFID reader

Setup settings for EVO 4.3 (EVO_Test_Leitfaden.aes)

File Communication Logfile Display Designer Manual

RFID reader

Device modes Date/Time Operation mode Camera Memory
 Basic settings Global variables RFID reader Fingerprint Timeboy

RFID reader type: Legic Advant (also Prime)

Global Default Config 1

Value-to-read Further configuration

Serial number Advant format at PrimeID card type

Free choice of data With segment: 1 Length

By search string 00000000000000000000000000000000 Length 13

Search String in hex values. (2 digits correspond to 1 byte length)
 Legic Prime length of the search string is limited to max. 7 byte.

Start/Offset at: 8 Count: 8

Additional options
 Without CRC check 8 Bit CRC 1 Address
 16 Bit CRC

Output format
 Decimal Fixed length: 8

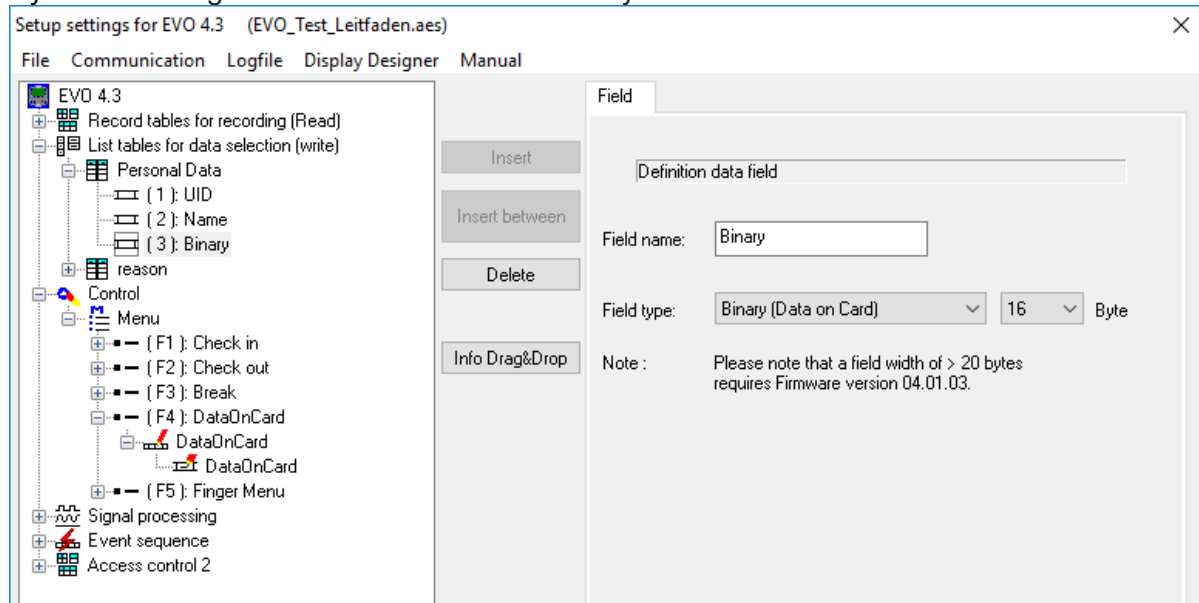
Note: For a fixed field length is filled with leading zeros.

OK

The transponder configuration for the reading can be freely selected. However, firstly it needs to be defined in the basic transponder settings.

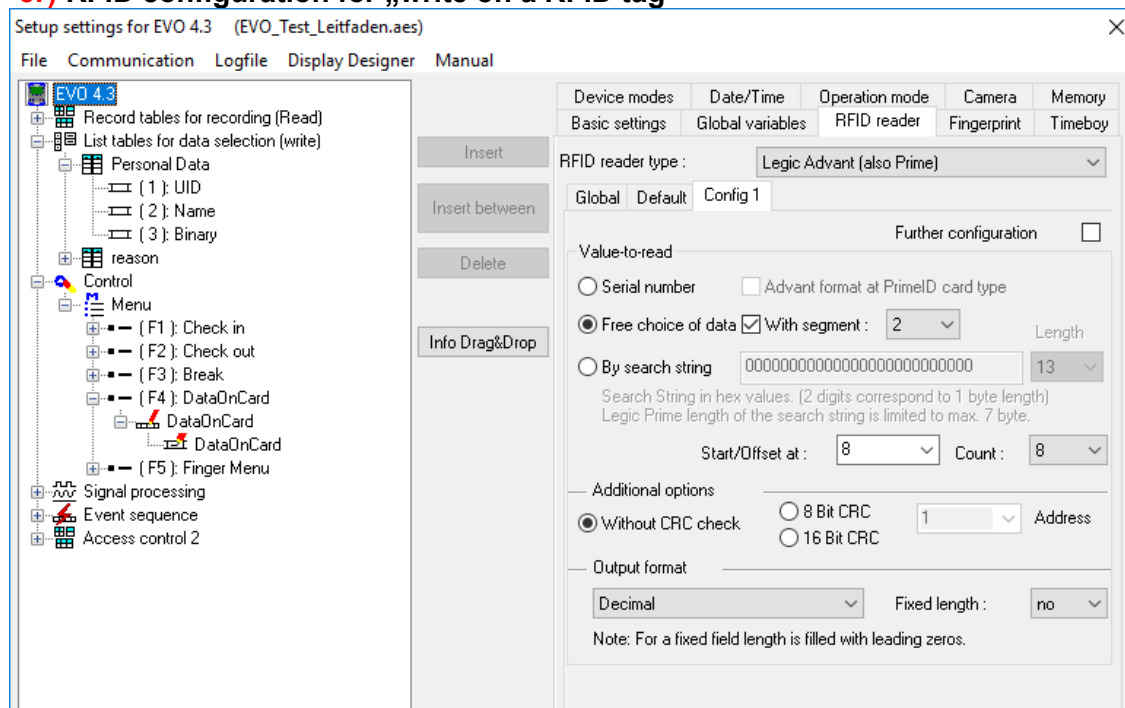
2.) List / binary file structure

By the list configuration the list who has a binary field will be selected.



In this example, the value of the transponder reading, who is wanted in the list in the ID field. The data that needs to be written is binary on the Data on Card field. The maximum field size is not allowed to exceed more than 220 bytes. After this, the further procedure can be set for list errors.

3.) RFID configuration for „write on a RFID tag”



The transponder configuration for the reading can be freely selected. However, firstly it needs to be defined in the basic transponder settings.



Please note:

First, complete the transponder configuration, then create the list with the binary field and finally parameterize the field function Data on Card.

Example for Data on Card:

ID with serial number: **1848989745**

List entry for **1848989745** in the file before transferring to the device

Field ID Field Data (binary field) here as hex bytes

1848989745 30313233343536373839414243444546303132333435363738394142434445463031323334353637383941

Data after conversion or within the device

Field ID Field Data (binary field) is binary here

1848989745 0123456789ABCDEF0123456789ABCDEF0123456789A

The following data will be written on the ID card:

0123456789ABCDEF0123456789ABCDEF0123456789A

Binary the data looks like this:

0x30, 0x31, 0x32, 0x33, 0x34



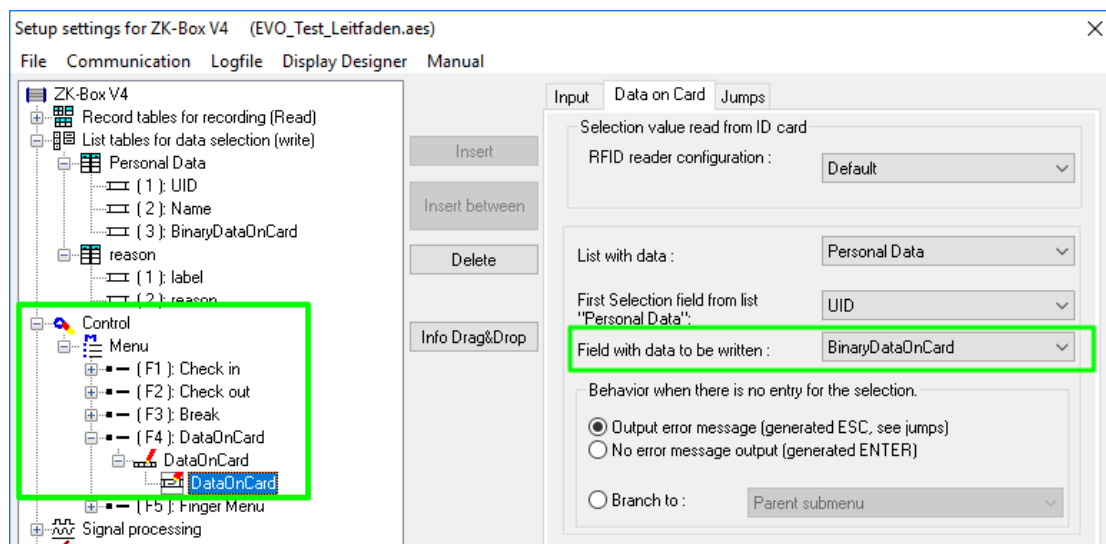
Please note:

When a 3-tone sequence is signaled, the Data-On-Card option is not available on this device. The option has to be purchased afterwards.

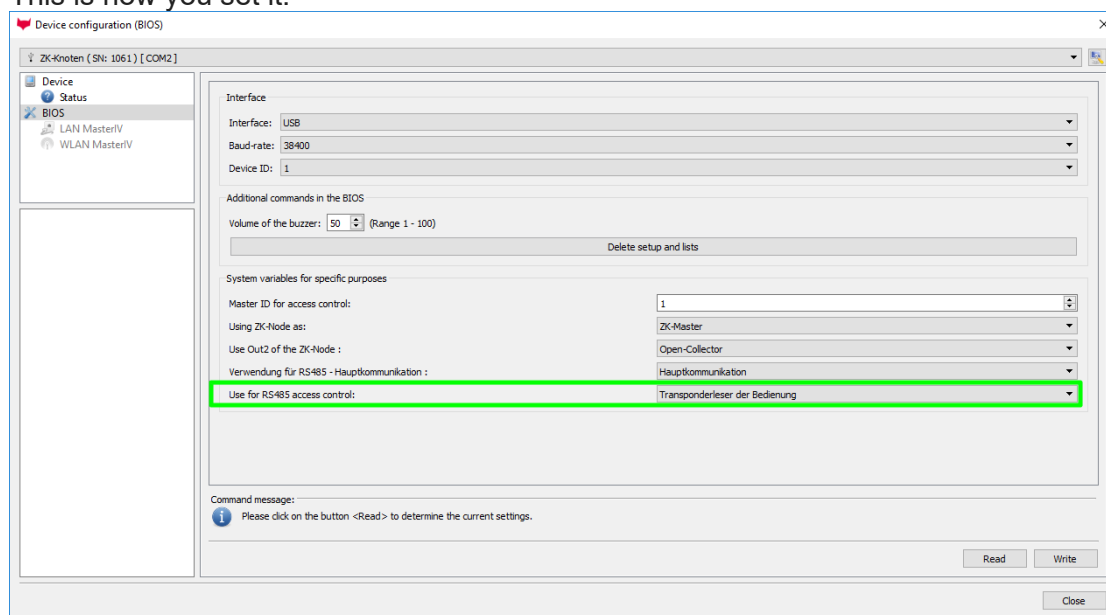
5.8.3. DataOnCard on the access control reader

In order to be able to use on a standard ZK reader of the EVO or the PHG series, the following settings must be made.

The functions for DataOnCard described in the previous chapters can only be set in the setup under Control menu.



Now it is necessary to be able to access the *access control reader* under the control. This is how you set it:



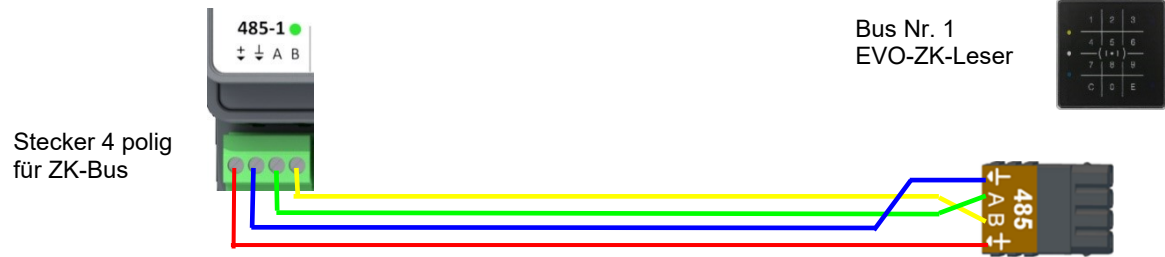
The reader on the *access control reader* (ZK) bus (RS485) is now activated via the Control menu (Operation transponder reader)

Please note:

Only one *access control reader* (ZK) can be connected to the bus at any time. Dip switch 1 and the termination of the bus must be set to "ON" (Bus address 1).

5.8.4. DataOnCard and a access control reader - wiring

Verdrahtungsplan für einen Busanschluss mit einem Intera 2:



6. technical data KYO Fourloc

KYO Fourloc Terminal V4.X

24.05.2023 EN | TECHNICAL DATA

Housing	Structure	plastic: PC/ABS UL94-V0
	Dimension	140 x 100 x 60 mm
	Weight (without power supply)	Standard device ca. 260 g
System	Clock	Real time clock
Data-storage	Flash	4 MB (optional 16 MB), 100.000 write cycles
	Memory expansion (optional)	SD card, max 2 GB
Display, keys	21 LEDs	Signalisation: 4x Status, 4x RS 485, 6x relay, 7x digital input
	2 keys	2 Keys, pushable trough pointed objects for special functions
Power	Power supply	12-24 V Directed Current (max. 8-30 V DC)
	PoE (optional)	PoE Module integrated (802.3bt, 802.3at oder 802.3af, Class 0)
	Power	Base unit without external devices ca. 1.5 W
	Clock / Ram buffering	Goldcap, backup of the time up to one day.
Environment values	Ambient temperature	-20 °C to +50 °C
	Protection	IP 20
Software	Configuration program	Setup program (Datafox-Studio) to configure without programming effort
	Communication tools	HTTP(S), library (DLL, so) or C++ source code to integrate into the application
Data transmission to PC/Server	USB	USB-C integrated
	TCP/IP	TCP/IP with integrated TCP/IP-Stack, 10/100 Mbit
	RS485	Access bus 4 may be used as RS-485 main communication
	WLAN (optional)	wireless LAN module integrated, WLAN 802.11 bgn (2.4GHz)
Access options	RS485 external	Connection of 4 access busses with up to 16 door modules / access readers per bus
	Relay	6 Relay changeover contact, 30V AC, 30V DC, 2A, max. 60 W
	Inputs	7 supervised inputs for connection of switch or relay, input shorted = input active
	Sabotage sensor	Tamper sensor can be connected to digital input

7. Index

A

Access 38

D

Device 16

DNS 28

F

For your Safety 1

H

Holiday Control 38

Holiday control ZK 38

I

Integration of a Burglar Detection System
(BDS) 74

Intended Use and Environmental Protection 5
introduction 2

K

Kommunikation 18

Umschalten 18

Kommunikation umstellen 30

L

LED 33

O

Office Mode 112

S

Switch Relays via time table: 38

System Requirements / Hardware 10

T

TCP/IP 21

technical data KYO Fourloc 123

U

UPS 12

USB 18, 20