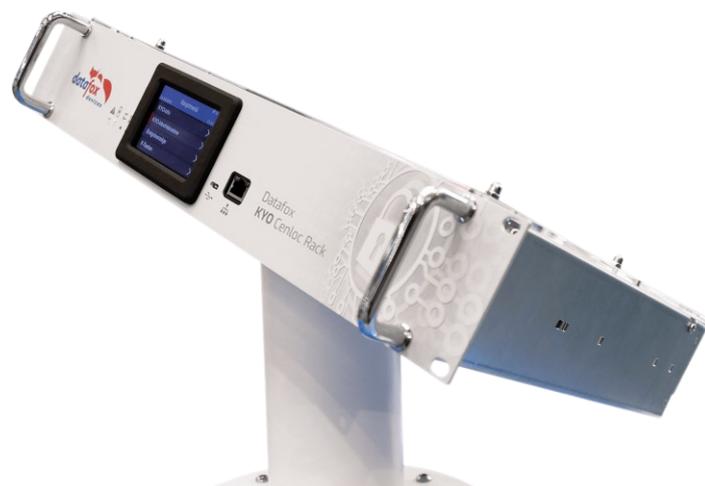




Datafox GmbH • Dermbacher Straße 12-14 • D-36419 Geisa • [www.datafox.de](http://www.datafox.de)

# Handbuch Datafox KYO Cenloc

Flexible Datenerfassung mit Methode



**© 2023 Datafox GmbH**

Dieses Dokument wurde von der Datafox GmbH erstellt und ist gegenüber Dritten urheberrechtlich geschützt. Die enthaltenen Informationen, Kenntnisse und Darstellungen betrachtet die Datafox GmbH als ihr alleiniges Eigentum. Alle Rechte, auch die der Übersetzung, des Nachdrucks oder der Vervielfältigung des gesamten Dokumentes oder Teile daraus, bedürfen der schriftlichen Zustimmung durch die Datafox GmbH. Die Geltendmachung aller diesbezüglichen Rechte, insbesondere für den Fall der Erteilung von Patenten, bleibt der Datafox GmbH vorbehalten. Die Übergabe der Dokumentation begründet keinerlei Anspruch auf Lizenz oder Benutzung der Soft- oder Hardware. Kopien der Disketten und CDs dürfen lediglich zum Zweck der Datensicherung angefertigt werden.

## Änderungen

### Änderungen in diesem Dokument

Datum	Kapitel	Beschreibung
13.05.2019	Alle	Neuaufgabe des Handbuches auf Versionstand 04.03.12.xx
09.10.2019	ZK-Anschlussvarianten	Kapitel ergänzt
04.11.2019	Alle notwendigen	Anpassung an Firmware 04.03.13.xx
01.05.2021	Alle notwendigen	Anpassung an Firmware 04.03.15.xx
013.09.2023	Alle notwendigen	Anpassung an Firmware 04.03.19.xx

### Versionsänderungen

Mit der Gerätegeneration IV wurde ein neues Versionierungssystem eingeführt. Nach diesem System setzt sich der Dateiname für die Gerätefirmware bzw. das Setupprogramm (Datafox StudioIV) wie folgt zusammen:

Produkt-bezeichnung	XX. Geräte-generation	YY. Kompatibilität (welche Versionen können zusammen eingesetzt werden)	ZZ. Versionsnummer (Funktionserweiterung)	Build Fehlerbeseitigung (mit einer neuen Version wird die Build-Nr. auf Null gesetzt)
z. B. PZE-MasterIV	04.	03.	12.	04

Die Verwendung des Handbuches richtet sich nach den verwendeten Versionen der Firmware und des DatafoxStudioIV bzw. der DFComDLL. Die Zusammengehörigkeit entnehmen Sie bitte den Hinweisen im Text.

**Firmware 04.03.19.xx , Studio und DLL Gültigkeit:** 04.03.21.xx.

Das DatafoxStudioIV ist abwärtskompatibel. D.h., Sie können mit einem neueren DatafoxStudioIV auch Geräte mit einem älteren Firmwarestand konfigurieren, wobei das Gerät natürlich nur die Funktionen unterstützt, die in dem älteren Firmwarestand realisiert sind. D.h., relevant für die Funktionen, die möglich sind, ist immer der Handbuchstand, der der Firmware mit dem zugehörigen Setup entspricht. Es ist nicht möglich, eine Firmware mit einem Stand des DatafoxStudioIV zu konfigurieren, der älter ist als die Firmware.

Empfehlung:

Verwenden Sie möglichst immer das aktuellste DatafoxStudioIV.

Welche Funktionen bei welchen Softwareständen unterstützt werden, ist ersichtlich in der Datei: Datafox MasterIV, SW-Versionsliste Stand xxx.pdf.

Die Datei befindet sich auf der Datafox DVD und zum Download auf der Homepage. Bitte beachten Sie weiterhin auch die Hinweise in den einzelnen Kapiteln im Handbuch. Die Updates stehen auf unserer Internetseite [www.datafox.de](http://www.datafox.de) unter Download zur Verfügung.

# Inhalt

<b>1.</b>	<b>Zu Ihrer Sicherheit</b>	<b>1</b>
<b>2.</b>	<b>Systemvoraussetzungen / Hardware</b>	<b>3</b>
<b>2.1.</b>	<b>Systemaufbau</b>	<b>3</b>
<b>2.2.</b>	<b>Installationsvoraussetzungen für den Betrieb der Datafox-Geräte</b>	<b>4</b>
<b>2.3.</b>	<b>Allgemeine Hardwareinformationen</b>	<b>5</b>
2.3.1.	Hardware Ausstattung	5
2.3.2.	Verhalten bei Stromausfall	5
2.3.3.	USV	5
<b>2.4.</b>	<b>Kompatibilität</b>	<b>7</b>
2.4.1.	Das Firmwaredateiarchiv (*.dfz)	7
2.4.2.	Datafox-Geräte und Geräte-Firmware	7
2.4.3.	Geräte-Firmware und Geräte-Setup	8
2.4.4.	Geräte-Firmware und Kommunikations-DLL	8
2.4.5.	Kommunikations-DLL und DatafoxStudioIV	8
2.4.6.	DatafoxStudioIV und Geräte-Setup	8
2.4.7.	Update / Downgrade	9
<b>3.</b>	<b>Gerät</b>	<b>11</b>
<b>3.1.</b>	<b>Inbetriebnahme</b>	<b>11</b>
<b>3.2.</b>	<b>Bedienung und Anzeigeelemente des KYO-Cenloc</b>	<b>13</b>
3.2.1.	Aufbau und Bedienung des KYO-Cenloc	13
3.2.2.	Display und Bios des KYO-Cenloc	13
3.2.2.1.	Aufbau Display Hauptmenü und Info-/ Funktionsmenüs	13
3.2.2.2.	KYO-Info	14
3.2.2.3.	Inbetriebnahme Datafox KYO Cenloc	17
3.2.2.4.	Inbetriebnahme-Modus für den Elektriker	18
3.2.2.5.	Aufbau Display Cenloc Bios-Menü	21
<b>3.3.</b>	<b>Kommunikationsarten der V4 Geräte</b>	<b>23</b>
3.3.1.	Kommunikation der V4 Geräte über USB	23
3.3.1.1.	Automatische Erkennung über USB für V4 Terminals	24
3.3.1.2.	USB Treiberinstallation für Datafox Geräte HW V4	25
3.3.2.	Kommunikation über TCP / IP	29
3.3.3.	Kommunikation TCP / IP über LAN	30
3.3.4.	Kommunikation TCP / IP über WLAN	31
3.3.4.1.	M111_WLAN ESP32-c3 ML01 (wLAN-Modul DF-WL03)	32
3.3.4.2.	Texas Instruments TI-CC3135 (Generation 2)	33
3.3.4.3.	Redpine (Generation 1)	34
3.3.4.4.	Einstellen der WLAN Parameter	35
3.3.4.5.	Verbindung der Terminals via TCP/IP DNS / DHCP	36
<b>3.4.</b>	<b>Anschluss KYO-Cenloc</b>	<b>39</b>
3.4.1.	Spannungsversorgung des KYO-Cenloc	40
3.4.1.1.	Spannungsversorgung 230V Netzanschluss	40
3.4.1.2.	Spannungsversorgung über POE	40
3.4.1.3.	Spannungsversorgung über den internen Akku	41
3.4.1.4.	Ausschalten des Gerätes und Wechsel des Akkus	41
3.4.1.5.	Spannungsversorgung über externe Spannungsquelle (DC)	42
3.4.1.6.	Anschluss der digitalen Eingänge	42
3.4.2.	Anschluss der digitalen Ausgänge auf der Hauptplatine	44
3.4.3.	Beschreibung der Erweiterungs-Module	45
3.4.3.1.	Anschluss eines Zutrittslesers an ein Erweiterungs-Modul	46
3.4.4.	Digitaler Eingang am Steck-Modul	52
3.4.4.1.	Anschluss eines Türöffners	53
<b>3.5.</b>	<b>Anschluss der Zutrittskontrolle</b>	<b>55</b>

3.5.1.	Konfiguration der ZK / Übersicht.....	55
3.5.2.	Beschreibung der Tabellen für die Zutrittskontrolle 2 .....	58
3.5.3.	Anschlussvarianten für den Datafox KYO Cenloc .....	61
3.5.3.1.	Sternförmiger Aufbau der ZK für den Datafox KYO Cenloc.....	61
3.5.3.2.	Sternförmiger Aufbau mit 4 Lesern .....	62
3.5.3.3.	2 x RS485 Bus, 4 Leser an 2 Tür innen/außen .....	67
3.5.4.	Hinweise für den Elektriker zur Installation der Zutrittskontrolle .....	71
3.5.4.1.	Busverkabelung Sternförmig.....	71
3.5.5.	Zutrittskontrolle II mit EVO Intera II .....	73
3.5.5.1.	EVO Intera II, Individuelle Einstellungen .....	77
3.5.6.	Zutrittskontrolle II mit EVO Agera.....	81
3.5.6.1.	Aufbau der Anzeigen und Bedienung.....	81
3.5.6.2.	Anzeigen für den ZK-Status .....	82
3.5.6.3.	Anzeigen einer PIN-Tastatur.....	82
3.5.6.4.	Fehlerausgaben.....	82
3.5.6.5.	Bios-Menü .....	83
3.5.6.6.	Allgemeine Konfiguration .....	83
3.5.6.7.	Display Konfiguration .....	84
3.5.6.8.	Bus Konfiguration .....	84
3.5.6.9.	Einstellen der Bus - Adresse.....	84
3.5.6.10.	Aktivierung des Bus - Abschlusswiderstands .....	84
3.5.7.	Funktionserweiterung für die Zutrittskontrolle 2.....	85
3.5.7.1.	Allgemeine Informationen .....	85
3.5.7.2.	Beispiele .....	85
3.5.7.3.	Tabelle <i>Time</i> .....	86
3.5.7.4.	Beschreibung der Tabelle „Action2“ .....	90
3.5.7.5.	Weitere Funktionen für ZK .....	91
3.5.7.6.	Liste Presence.....	92
3.5.8.	Anbindung EMA (Einbruchmeldeanlage) .....	93
3.5.8.1.	Konfigurieren der EMA in der Zutrittskontrolle.....	93
3.5.8.2.	Relais und digitale Eingänge zur Steuerung (Type 2) .....	94
3.5.8.3.	Definition der Codes zum Ein- und Ausschalten (Type 3) .....	95
3.5.8.4.	Zuordnung der Leser zu EMA-Bereichen (Type 4).....	96
3.5.8.5.	Ausweise zur EMA-Schaltung berechtigen .....	97
3.5.8.6.	Statuscodes.....	98
3.5.8.7.	Aktivierungsablauf im Controller .....	99
3.5.9.	Automatische Relaisabschaltung nach Öffnung der Tür.....	101
3.5.9.1.	Überwachte Türen .....	101
3.5.9.2.	Konfiguration der überwachten Tür .....	102
3.5.9.3.	Aufbau des Eintrags in der ReaderProps Liste .....	102
3.5.9.4.	Prüfung der Türmodule in der Zutrittskontroller .....	102
3.5.9.5.	Sonderfall zeitlich gesteuerte Relais .....	103
3.5.9.6.	Beispiel Konfiguration .....	103
3.5.10.	Statusmeldungen der Zutrittskontrolle.....	105
3.5.11.	Statusanzeige der Zutrittsmodule über LEDs.....	110
3.5.12.	Onlinefunktionen der Zutrittskontrolle.....	111
3.5.12.1.	Online über HTTP-Anbindung.....	111
3.5.12.2.	Online über DLL-Anbindung .....	114
3.5.13.	Online/Offline-Zutrittskontrolle mit Vorprüfung .....	115
3.5.13.1.	Konfiguration der Online/Offline-Zutrittskontrolle mit Vorprüfung.....	115
3.5.13.2.	Einstellungen im Setup .....	115
3.5.13.3.	Betriebsmodus der Zutrittskontrolle ermitteln .....	115
3.5.13.4.	Ablauf der Online/Offline-Zutrittskontrolle mit Vorprüfung .....	115
3.5.13.5.	Quittierung des Vorprüfungsdatensatzes .....	116
3.5.13.6.	HTTP-Schnittstellen: Methode df_ao_ac2.....	116
3.5.13.7.	DLL-Funktion: DFCQuitRecordExt().....	117

3.5.13.8.	Sonderfall: Identifikation nicht möglich .....	118
3.5.14.	Funktionen für ZK und U&Z .....	119
3.5.14.1.	Aufbaubeispiel .....	119
3.5.14.2.	Inbetriebnahme der Schließzylinder .....	122
3.5.14.3.	Montage und Demontage der Zylinder .....	122
3.5.14.4.	Einrichten des Funknetzwerkes .....	123
3.5.14.5.	Batteriewechsel / Status / Lebensdauer .....	124
3.5.14.6.	Wechseln der ZK-Master ID / Knob Active Time .....	125
3.5.14.7.	Optische und akustische Signale des U&Z Schließzylinders .....	126
3.5.14.8.	Optische und akustische Signale des U&Z Türdrückers .....	127
3.5.14.9.	Zurücksetzen des U&Z Schließzylinders .....	127
3.5.14.10.	Hinweise zum Service Key .....	128
3.5.14.11.	Unterstützte Transponderverfahren und Einschränkungen .....	129
3.5.14.12.	Servicekey beschädigt / verloren .....	130
3.5.14.13.	Servicekey ersetzen .....	130
3.5.14.14.	Technische Daten des Funkmoduls .....	130
3.5.15.	Dauer-Öffnung bei Uhlmann&Zacher Funkbeschlägen .....	131
3.5.16.	U&Z-Dauer-Öffnung einer Tür (Variante 1 – Sicherer Betriebsmodus) .....	131
3.5.16.1.	Aktivieren der Daueröffnung .....	131
3.5.16.2.	Bedienung während Dauer-Öffnung .....	131
3.5.16.3.	Rücknahme einer Dauer-Öffnung .....	132
3.5.16.4.	Zusammenfassung .....	132
3.5.17.	U&Z-Dauer-Öffnung einer Tür (Variante 2 – Klassischer Modus) .....	133
3.5.17.1.	Daueröffnung mithilfe des klassischen Modus .....	133
3.5.17.2.	Einrichten der Daueröffnung mithilfe des klassischen Modus .....	133
3.5.17.3.	LED- und Buzzer-Signalisierungen des Zylinders im klassischen Modus .....	134
3.5.18.	Bedienung /Aktivierung-Deaktivierung des Office-Mode .....	135
3.5.18.1.	Aktivierung .....	135
3.5.18.2.	Deaktivierung .....	135
3.5.18.3.	Hinweise .....	136
<b>4.</b>	<b>Technische Daten KYO Cenloc</b>	<b>137</b>
<b>5.</b>	<b>Index</b>	<b>138</b>

## 1. Zu Ihrer Sicherheit

### Sicherheitshinweise für den Umgang mit den Datafox Produkten



Das KYO Cenloc darf nur bestimmungsgemäß entsprechend den Angaben im Benutzerhandbuch betrieben werden. Führen Sie keinerlei Fremdgegenstände in Öffnungen und Anschlüsse ein. Das Gerät darf nicht geöffnet werden. Sämtliche Wartungs- und Instandsetzungsarbeiten dürfen nur durch autorisiertes Fachpersonal durchgeführt werden.



Manche Geräte enthalten einen Lithium-Ionen Akku oder eine Lithium Batterie.  
Nicht ins Feuer werfen!

Stromversorgung: 12 Volt DC  
Siehe jeweiliges Typenschild / technische Daten.  
Das Gerät darf extern nur mit einer leistungsbegrenzten Stromquelle nach EN 60950-1 betrieben werden. Werden diese Hinweise nicht eingehalten, kann das zur Zerstörung des Gerätes führen.  
Folgende Temperaturbereiche sind zu beachten:  
Arbeitsbereich / Lagertemperatur: -20° C bis +60° C  
Mit Mobilfunkmodem: 20° C bis +55° C

#### Achtung!



In Bereichen, in welchen Handyverbot besteht, müssen Mobilfunk und WLAN und gegebenenfalls auch andere Funkmodule abgeschaltet werden.  
Träger von Herzschrittmachern:  
Halten Sie bei der Benutzung des Gerätes einen Sicherheitsabstand von mindestens 20 cm zum implantierten Herzschrittmacher ein, um eventuelle Störungen zu vermeiden. Schalten Sie das Gerät sofort aus, wenn Beeinträchtigungen zu vermuten sind.

**Schutzklasse:** Beachten Sie die technischen Daten zum jeweiligen Gerät.



Bei Lasergeräten der Klasse 2 ist das Auge bei zufälligem, kurzzeitigem Hineinschauen in die Laserstrahlung durch den Lidschlussreflex und/oder Abwendreaktionen geschützt. Diese Geräte dürfen deshalb ohne weitere Schutzmaßnahmen eingesetzt werden. Trotzdem sollte man nicht in den Laserstrahl des Laserscanners blicken.

**Beachten Sie die zusätzlichen Hinweise im Kapitel.**  
**[„Bestimmungsmäßiger Gebrauch und Umweltschutz“.](#)**

Wir erklären in alleiniger Verantwortung, dass das bezeichnete Produkt die Schutzanforderungen der Europäischen Richtlinie 89/336/EWG, geändert durch 91/236/EWG, 92/31/EWG, 93/97/EWG und 93/68/EWG, erfüllt. Der Nachweis erfolgt durch die Einhaltung der folgenden Normen:



- 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. Systemvoraussetzungen / Hardware

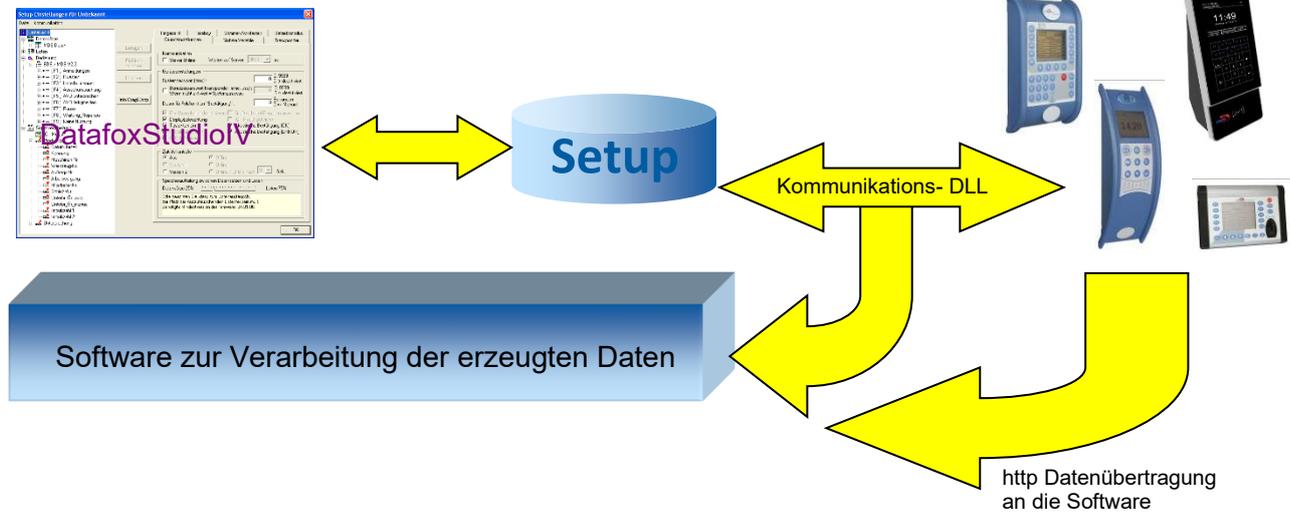
### 2.1. Systemaufbau

Das System setzt sich aus dem Datafox Gerät, dem DatafoxStudioIV, des Übertragungsweges Kommunikations DLL oder http und einer Software zur Verarbeitung der erzeugten Daten zusammen.

#### Setuperstellung

#### Setup speichern

#### Setup auf Gerät übertragen



## 2.2. Installationsvoraussetzungen für den Betrieb der Datafox-Geräte

### Installationsvoraussetzungen

Sie benötigen einen 230 V Netzanschluss für das Datafox Gerätenetzteil oder POE, um das Datafox Gerät in Betrieb zu nehmen. Je nach eingestellter Hauptkommunikation benötigen Sie ein entsprechendes Übertragungsmedium bzw. Anschlussleitung.

Hauptkommunikation:

- USB > ein Standard USB-A auf USB-Mirco Kabel (siehe Anschluss USB).
- RS485 > eine dem EIA-485 Standard entsprechende Übertragungsstrecke (siehe Anschluss RS485).
- 2G; 4G > eine störungsfreie Mobilfunkverbindung.
- WLAN > einen störungsfreien Funkkanal zu einem Access Point (802.11 b/g/n) in Reichweite (siehe Anschluss WLAN).
- TCP/IP > min. ein Standard Ethernet Kabel, kein „cross over“ (RJ 45 Stecker).
- HTTP(Internet) über LAN > TCP/IP-Anschluss mit freiem Internetzugang. Die Daten werden dann an einen Server gesendet.

Idealerweise sollte die Kabel in einer Unterputzdose Bereit gestellt werden. Beachten Sie hierzu bitte die Höhenangabe in der [Montageanleitung](#).

Montagealleitungen auf unsere 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/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/Datafox EVO 3.5 Universal EVO Agera Montagezeichnung.pdf](https://www.datafox.de/d67/unternehmen/downloads/informationsmaterial/evo-3-5-universal/Datafox_EVO_3.5_Universal_EVO_Agera_Montagezeichnung.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/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/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-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/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](https://www.datafox.de/d67/unternehmen/downloads/informationsmaterial/pze-master-iv/105406_Datafox_PZEMIV_Wandhalterung_Montageanleitung.pdf)



### Hinweis:

Mit steigenden Anforderungen hinsichtlich Übertragungsrates und Störsicherheit steigen auch die Anforderungen an die Übertragungsstrecke hinsichtlich Güte (Störfestigkeit).

## **2.3. Allgemeine Hardwareinformationen**

### **2.3.1. Hardware Ausstattung**

Die Geräte der Hardware V4 sind mit einem Flash-Speicher ausgestattet. Je nach Gerätetyp bzw. gewählter Option mit 4 oder 16 MB.

Für die Daten wird der Speicher als quasi Ringspeicher verwendet. Wird der komplette Ringspeicher beschrieben ohne dass die Daten abgerufen werden, meldet das Terminal „Speicher voll“, bitte Admin benachrichtigen“. In dieser Zeit werden keine weiteren Daten gespeichert.

Daten die bereits gelesen wurden, werden so nach und nach überschrieben. Es wird immer mit dem gesamten Speicher gearbeitet, um die Zugriffe pro Speicherzelle zu minimieren.

Es kommt ein ARM-Mikrokontroller mit 32 Bit Technologie zum Einsatz.

Je nach Gerätetyp hat das Gerät einen Goldcap Kondensator zur Pufferung der Uhrzeit. Dieser gewährleistet, dass die Uhr bei Unterbrechung der Spannungsversorgung noch bis zu einer Woche korrekt weiterläuft.

In anderen Geräten, wie EVO 4.3, PZE- AE-Master V4 und KYO Cenloc ist zusätzlich zum Kondensator noch eine Pufferbatterie eingebaut. Mit dieser hält die Uhr ca. 4 Jahre ihren Wert auch ohne externe Spannungsversorgung.

Die genaue Ausstattung finden Sie im letzten Kapitel Technische Daten.

### **2.3.2. Verhalten bei Stromausfall**

Das Gerät bootet nach dem Wiedereinschalten der Spannungsversorgung automatisch.

Alle Daten, die vor dem Stromausfall noch nicht versendet oder von der Anwendungssoftware noch nicht abgeholt wurden, werden auf dem Gerät gespeichert.

Diese gehen nicht verloren. Nach dem Booten stehen diese Daten wieder zur Verfügung.

### **2.3.3. USV**

Der KYO-Cenloc kann optional mit einem Bleiakku versorgt werden.

Siehe hierzu mehr im Kapitel „[Spannungsversorgung über internen Akku](#)“.



## 2.4. Kompatibilität

Die Kompatibilität ist zwingend zu beachten zwischen:

- Datafox-Gerät und der Geräte-Firmware
- Geräte-Firmware und Geräte-Setup
- Geräte-Firmware und Kommunikations-DLL
- Kommunikations-DLL und DatafoxStudioIV
- DatafoxStudioIV und Geräte-Setup

### 2.4.1. Das Firmwaredateiarchiv (\*.dfz)

#### Beschreibung

Gerätedateien (\*.hex) der Master – Geräte, werden in einem gemeinsamen Firmwaredateiarchiv ausgeliefert. Dieses besitzt die Endung dfz (steht für Datafox Zip). Statt wie bisher die Gerätedateien (\*.hex), werden nun einfach die Firmwaredateiarchive (\*.dfz) angegeben. Dies gilt für das DatafoxStudioIV und die DLL. Die Angabe der Gerätedateien (\*.hex) ist weiterhin möglich.

#### Funktion des Archives

Auf Grundlage der im Gerät vorliegenden Hardwareoptionen sucht die Übertragungsroutine der Gerätedatei die passende Gerätedatei aus dem Firmwaredateiarchiv aus. Somit wird sichergestellt, dass auch alle im Gerät verfügbaren Hardwarekomponenten von der entsprechenden Firmware unterstützt werden.

#### Manuelle Auswahl einer Datei

Falls Sie im Rahmen Ihrer Installation nicht das Archiv einbinden wollen, haben Sie die Möglichkeit einzelne Gerätedateien aus dem Archiv in Ihre Installation zu übernehmen.

Das zugrunde liegende Dateiformat des Firmwaredateiarchivs ist Zip. Somit können Sie das Archiv mit jedem handelsüblichen Zip-Programm öffnen. Über das Kommando „Öffnen mit“ des Kontextmenüs, können Sie ein entsprechendes Programm zum Öffnen wählen. Ggf. können Sie durch Umbenennung der Dateiendung von dfz auf zip ein mit der Endung verknüpftes Programm aufrufen, um die Datei zu öffnen.

In dem Archiv finden Sie eine Datei mit dem Namen „Inhalt.pdf“. Aus dieser können Sie entnehmen, welche Datei (\*.hex) des Archivs zu Ihrem Gerät passt. Bitte extrahieren Sie die gewünschte Gerätedatei (\*.hex) und benennen diese ggf. um. Eine Umbenennung der Datei ist jederzeit möglich, da alle Informationen in der Datei selbst vorliegen.

Die zuvor extrahierte Gerätedatei können Sie im DatafoxStudioIV, sowie bei Aufruf der DLL-Funktion als Gerätedatei angeben. Vor der Übertragung wird nach wie vor geprüft, ob die Datei auch in das gewählte Gerät eingespielt werden kann.

### 2.4.2. Datafox-Geräte und Geräte-Firmware

Jedes Datafox-Gerät besitzt eine elektronische Flachbaugruppe. Diese wiederum besitzt eine spezifische Hardwareausstattung bzgl. der Optionen (z. B. Mobilfunk, WLAN, Fingerprint, ...). Aufgrund technischer Gegebenheiten, schließen sich verschiedene Optionen gegenseitig aus. Zudem ist es durch den begrenzten Programmspeicher derzeit nicht möglich, alle Hardwareoptionen in einem Firmware File zu unterstützen. Das heißt, jedes Gerät mit spezifischen Hardwareoptionen benötigt eine passende Firmware, um die Hardwareoptionen softwaretechnisch zu unterstützen.



#### **Achtung:**

Ab DatafoxStudioIV Version 04.02.00.x wird die Hardwaregeneration V 3 unterstützt. Dabei ist das DatafoxStudioIV kompatibel bis einschließlich Firmware Version 04.01.x.y. Ältere Versionen 04.00.x.y werden nicht mehr unterstützt.

### 2.4.3. Geräte-Firmware und Geräte-Setup

Die Firmware (Betriebssystem) des Gerätes und das Geräte-Setup (\*.aes Datei = Anwendungsprogramm) bilden eine Einheit. Mit dem Geräte-Setup wird festgelegt, wie sich das Gerät (die Firmware) zur Laufzeit verhalten soll. Das heißt, wie das Gerät auf Eingabeereignisse durch den Anwender oder die Umgebung (z. B. digitale Eingänge) reagiert. Grundsätzlich werden nur die Funktionen des Gerätes ausgeführt, die von der Firmware unterstützt werden und über das Setup definiert sind. Daher sollten Sie jedes Setup vor der produktiven Inbetriebnahme mit dem zugehörigen Gerät bzw. auf einem Gerät mit gleichen Hardwareoptionen und gleicher Firmware testen.

### 2.4.4. Geräte-Firmware und Kommunikations-DLL

Wie wir bereits festgestellt haben, unterstützt eine Firmware bestimmte Funktionen in Abhängigkeit von den Hardwareoptionen. Die Kommunikations-DLL ist die Schnittstelle zwischen der Firmware und dem DatafoxStudioIV oder Ihrer Verarbeitungssoftware. Die Firmware muss daher immer die gleiche Versionsnummer wie die Kommunikations-DLL oder eine niedrigere Versionsnummer besitzen, also älteren Datums sein.

#### Hinweis:



Verwenden Sie in Ihrer Anwendung eine aktuellere Version der DLL als die Firmware, so können Sie nur Funktionen verwenden, welche die Firmware auch unterstützt.

Andernfalls erhalten Sie eine Fehlermeldung (z.B. Funktion wird nicht unterstützt) und diese ist dann abzufangen bzw. auszuwerten.

### 2.4.5. Kommunikations-DLL und DatafoxStudioIV

#### Hinweis:



Das DatafoxStudioIV und die Kommunikations-DLL werden in einem Bundle entwickelt und freigegeben und müssen daher im Bundle zum Einsatz kommen. Eine neue Version des DatafoxStudioIV, arbeitet nicht mit einer älteren DLL.

### 2.4.6. DatafoxStudioIV und Geräte-Setup

Mit dem DatafoxStudioIV wird ein Geräte-Setup (Anwendungsprogramm) für das Datafox-Gerät erstellt. Das heißt, nur die Funktionen, die in der DatafoxStudioIV Version zum Zeitpunkt der Erstellung zur Verfügung standen, wurden auch im Setup definiert. Das DatafoxStudioIV, mit dem Sie ein Geräte-Setup öffnen wollen, darf demzufolge höchstens aktueller sein, als die DatafoxStudioIV Version mit der das Geräte-Setup erstellt wurde, jedoch nicht älter.

#### Hinweis:



Updates stehen immer auf unserer Homepage [www.datafox.de](http://www.datafox.de) zum Download zur Verfügung.

#### Achtung:



Bei Auslieferung neuer Geräte wird immer die aktuelle Firmware auf die Geräte geladen. Wenn Sie mit einer älteren Firmware-Version arbeiten wollen, führen Sie ein Downgrade durch. Beachten Sie unbedingt die Kompatibilitätshinweise aus der Release-Note der jeweiligen Firmware Version.

Welche Funktionen mit welchem Softwarestand unterstützt werden, ist aus der Datei: <Gerätename>, Software Versionen Stand <Versionsnummer>.pdf ersichtlich. Die Datei befindet sich auf der Produkt-DVD. Bitte beachten Sie weiterhin auch die Hinweise in den einzelnen Kapiteln im Handbuch.

### 2.4.7. Update / Downgrade

Ein Firmware Update bzw. Downgrade ist ein sensibler Prozess, bei dem es unter Umständen zu einem Rücksetzen der Hauptkommunikation auf RS232 kommen kann. In jedem Fall sind die Angaben zur Kompatibilität in der Softwareversionsliste zu beachten.

#### Firmware Update



**Achtung:**

Bevor Sie ein Firmware-Update durchführen, prüfen Sie anhand der Softwareversionsliste, ob es Versionsabhängigkeiten gibt, die unbedingt einzuhalten sind.

Zum Beispiel muss bei einem Wechsel von der Version 04.00.xx auf die Version 04.01.xx als Mindestanforderung eine Version 04.00.23.769 oder höher vorliegen, um das Update erfolgreich auf die Version 04.01.xx durchführen zu können.

#### Firmware Downgrade

Eine Downgrade der Firmware ist nicht zu empfehlen.

Da wir ständig an der Verbesserung der Software/Firmware arbeiten, sind immer alle Funktionalitäten in die neuen Versionen übernommen. Neue Software bietet immer eine bessere Funktionalität und es sind evtl. Bugs behoben.



**Achtung:**

Bei einem Firmware-Downgrade ist die Firmware aus technischen Gründen immer zweimal auf das Gerät zu übertragen. Fehler in der Displayanzeige des Gerätes nach der ersten Übertragung können ignoriert werden.



### 3. Gerät

**Hinweis:**

Da Kunststoffe generell nicht 100%ig UV-beständig sind, muss auf einen geeigneten Schutz vor direkter Sonneneinstrahlung geachtet werden. Das Ausbleichen ist lediglich ein optischer Mangel, der die Funktionstüchtigkeit in keiner Weise einschränkt.

**Achtung:**

Bitte beachten Sie, dass in den MasterIV-Geräten ein Flash-Speicher zum Einsatz kommt. Laut Hersteller kann jeder Speicherblock (512 Byte) max. 100.000-mal beschrieben werden. Die Firmware der Geräte verteilt die Zugriffslast auf die einzelnen Speicherblöcke und markiert intern defekte Blöcke. Es ist jedoch trotz dieses Sicherheitsmechanismus von allzu häufiger Übertragung und allzu häufigem Editieren der Listendaten abzuraten. Die Applikation sollte nur bei Änderung neu übertragen werden. Auch Listen sollten nur neu übertragen werden wenn diese geändert wurden. Von einer zyklisch permanenten Übertragung ist abzuraten.

Bitte beachten Sie in diesem Zusammenhang den Hinweis „FlashService“ in der Displayanzeige des Gerätes, der Sie darauf aufmerksam macht, dass die laut Hersteller angegebene Lebensdauer des Flash-Speichers bald erreicht ist. Das Gerät ist dann zum Datafox Service einzusenden.

#### 3.1. Inbetriebnahme

Das Gerät ist bei Auslieferung voll funktionsfähig und mit einem Demo-Setup vorkonfiguriert, sodass Sie sofort die Eingabe testen können. Nach dem Herstellen der Stromversorgung schaltet sich das Gerät automatisch ein. Das Gerät startet automatisch den Bootvorgang, Erkennung der Hardwareoptionen und Laden des Setups. Nach Abschluss des Bootvorgangs wechselt das Gerät automatisch in die Bedienung. Der KYO Cenloc ist nun einsatzbereit.

**Hinweis:**

Bei Auslieferung steht die Hauptkommunikation auf USB bis zur Firmware 04.03.07.XX. Ab der Firmware 04.03.09.XX steht die Hauptkommunikation auf TCP/IP wenn das Gerät damit ausgestattet ist. Dabei ist DHCP aktiviert. Wird nun USB am PC angeschlossen, schaltet das Gerät automatisch auf USB um.

**Achtung:**

Kommen externe Module (z.B. Zutrittskontrolle, Signalverarbeitung über die digitalen Eingänge) mit einer externen Spannungsversorgung zum Einsatz, vergewissern Sie sich, dass alle Grenzwerte (max. Spannung und Strom) eingehalten wurden, bevor Sie das System in Betrieb nehmen.



## 3.2. Bedienung und Anzeigeelemente des KYO-Cenloc

### 3.2.1. Aufbau und Bedienung des KYO-Cenloc

Der KYO-Cenloc (Zutrittszentrale) verfügt über ein 3.5 Zoll Display mit kapazitiven Touch. Hier können direkt Einstellungen vorgenommen werden wie:

- IP-Adresse eingeben
- Port eingeben
- etc.

Weiter können vielfältige Informationen über den Zustand der angeschlossenen Leser, den Zustand der digitalen Ein- und Ausgänge abgefragt oder Ausgänge geschaltet werden.

Wie und wo Sie die Einstellungen vornehmen können, zeigen Ihnen die nachfolgenden Seiten.



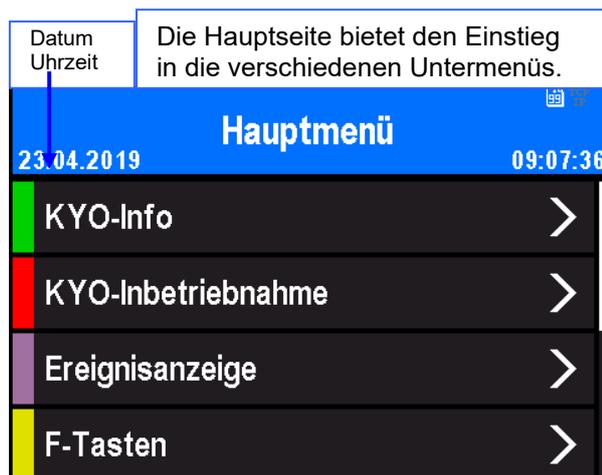
Display und Touchbereich

Wie Sie es von einem Smartphone gewöhnt sind, können Sie die nächste Seite durch Gestensteuerung nach oben verschieben. Dies gilt auch für Untermenüs.

### 3.2.2. Display und Bios des KYO-Cenloc

#### 3.2.2.1. Aufbau Display Hauptmenü und Info-/ Funktionsmenüs

Die gesamte Displayfläche ist mit einem Touch versehen. Tippen Sie einfach mit dem Finger auf die jeweilige Kachel, welche Sie anwählen möchten.



**KYO-Info:**

Hier kann der Zustand der digitalen Ein-/Ausgänge und der angeschlossenen Leser eingesehen werden.

**KYO-Inbetriebnahme:**

Dieses Menü dient ausschließlich zu Inbetriebnahme durch den Errichter. Hier können alle angeschlossenen Geräte getestet werden.

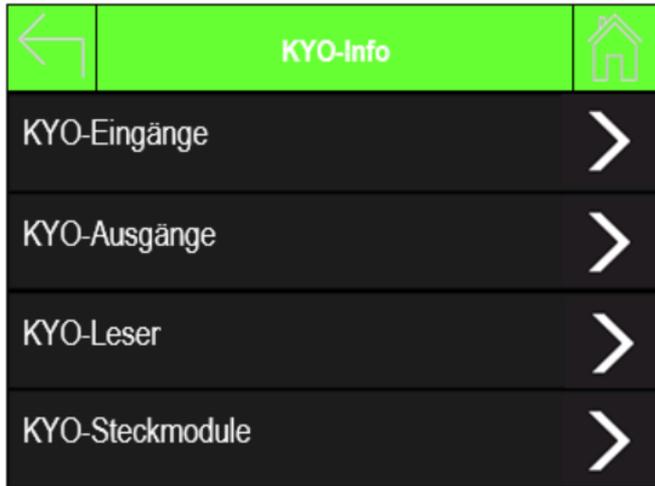
**Ereignisanzeige:**

Hier kann der Zustand der digitalen Ein-/Ausgänge und der angeschlossenen Leser eingesehen werden.

**F-Tasten:**

Mittels DatafoxStudioIV können hier Funktionen (Setup) ausgeführt werden. Konform zu den PZE-Geräten.

### 3.2.2.2. KYO-Info



#### KYO-Eingänge:

Anzeige der digitalen Eingänge:



#### KYO-Eingänge:

Hier am Beispiel Eingang 3 liegt auf „Low“ Signal. Das bedeutet, dass der Eingang auf Masse gebrückt ist.

#### KYO-Eingänge:

Hier am Beispiel Eingang 4 liegt auf „High“ Signal. Keine Brücke zur Masse.

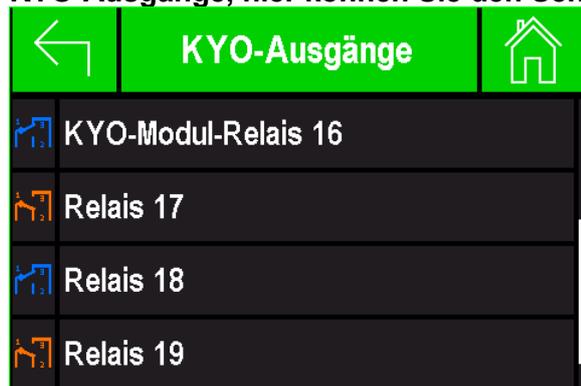
Letzte Seite:



#### KYO-Eingänge:

Digitale Eingänge auf der Hauptplatine. Hier am Beispiel Eingang 23 liegt auf „Low“ Signal. Das bedeutet, dass der Eingang auf Masse gebrückt ist.

KYO-Ausgänge, hier können Sie den Schaltzustand der Relais einsehen:



**KYO-Ausgänge:**  
Hier am Beispiel Relais auf dem Aufsteckmodul Platz 16 Relais ist ausgeschaltet.

**KYO-Ausgänge:**  
Hier am Beispiel Relais 17, Relais ist eingeschaltet.

KYO-Leser, hier sehen Sie alle am KYO-Cenloc angeschlossenen Leser.



**KYO-Leser:**  
Leser „Fehler“. Hier im Bsp.: Der Typ Falsch Statt Mifare wurde ein Legic angeschlossen.

**KYO-Leser:**  
Leser „Fehler“. Hier im Bsp.: Der Leser wurde nicht in der Reader-Liste eingetragen. Grund hierfür kann eine falsch eingestellte Busnummer sein.

Sie können sich über die Pfeiltasten **rechts** ▶-links ◀ die Infos über den nächsten Leser anschauen.

Info über den Leser: **Status 7**



Info: **Status 3**



nächste Seite

## KYO-Steckmodule:

Die Modulplätze 13-16 sind nicht bestückt.

← KYO-Steckmodule →				
-- = an diesem Platz kein Modul erkannt				
--	12	8	4	
--	11	7	3	
--	10	6	2	
--	9	5	1	

Hier sind alle Module bestückt:

← KYO-Steckmodule →				
-- = an diesem Platz kein Modul erkannt				
	16	12	8	4
	15	11	7	3
	14	10	6	2
	13	9	5	1



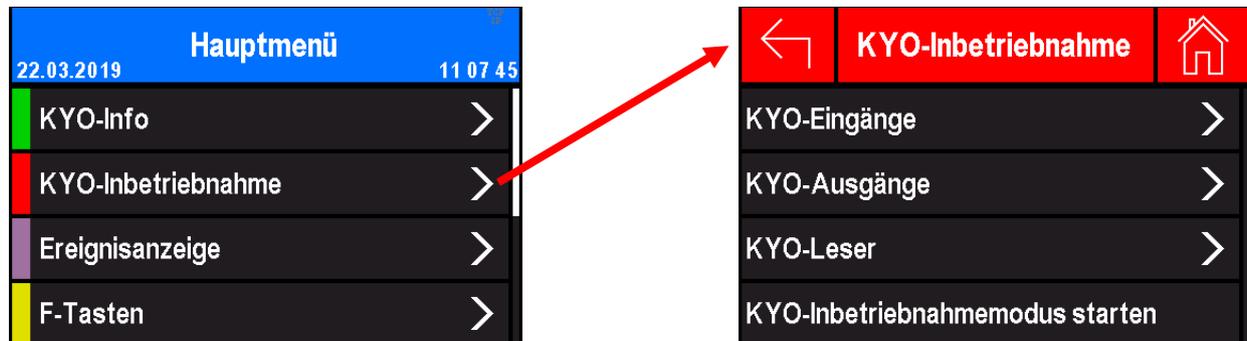
### Hinweis:

Wir empfehlen die Bestückung immer mit der Modulplatznummer aufsteigend vorzunehmen.

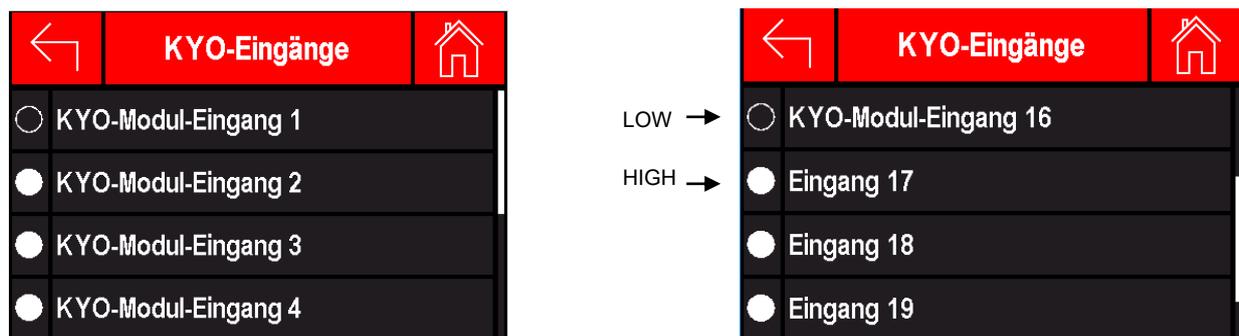
### 3.2.2.3. Inbetriebnahme Datafox KYO Cenloc

#### Ersteinrichtung des Datafox KYO Cenloc

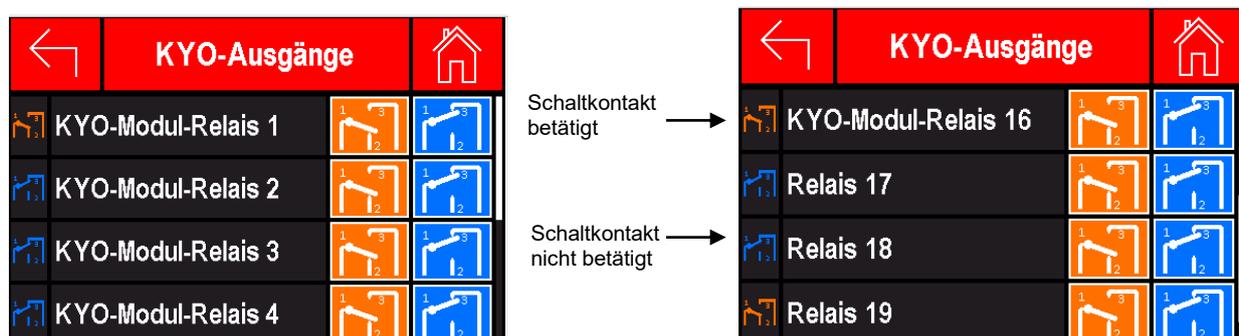
Für die Inbetriebnahme des Datafox KYO Cenloc nach Anschluss aller Peripherien muss zuerst ein Setup mit entsprechendem Zutrittslisten- und eventuell Datensatzaufbau eingespielt werden. Hierbei muss in der Reader-Liste zuerst einmal der Zutrittsmaster initialisiert sein. Nun kann man im Inbetriebnahme-Menü des KYO Cenloc die Einstellungen der angeschlossenen Busteilnehmer, den Zustand der Eingänge einsehen, Ausgänge direkt aus dem Menü heraus schalten und deren Funktionalität testen.



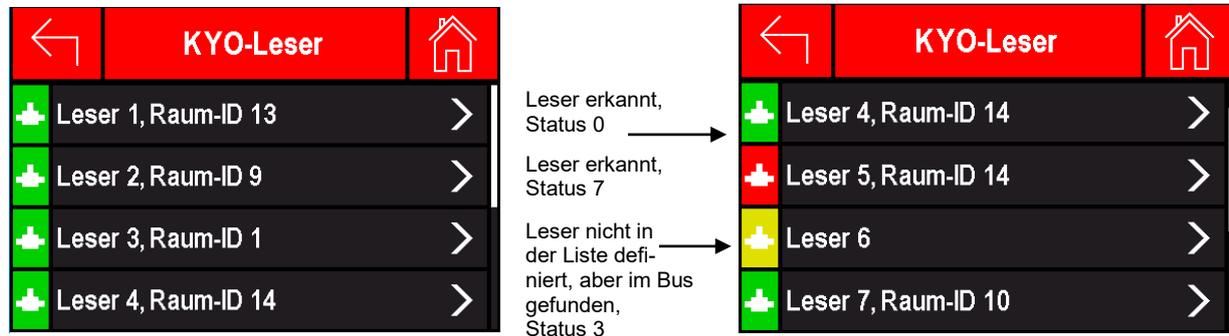
Im Menüpunkt KYO-Eingänge werden alle digitalen Eingänge im KYO Cenloc aufgelistet. Der aktuelle Zustand wird direkt im Display des KYO Cenloc über ein Symbol angezeigt. Bei nicht ausgefülltem Kreis liegt der Eingang auf LOW-Signal, ein ausgefüllter Kreis signalisiert ein HIGH-Signal am Eingang. Durch Scrollen am Display gelangt man durch die Übersicht und kann sich alle Eingänge anschauen.



Der Menüpunkt KYO-Ausgänge liefert den Zustand aller Relaisausgänge des KYO Cenloc. Durch Tippen auf die Schaltstellungen auf der rechten Seite kann man die Schaltkontakte der einzelnen Relais umschalten und die angeschlossene Hardware testen.



Durch Tippen auf KYO-Leser werden alle an die KYO-Module angeschlossenen Zutrittsleser aufgelistet und deren Buseigenschaften, sowie die Seriennummer und der zuletzt gelesene Transponder angezeigt. Ist ein Zutrittsleser nicht in den Zutrittslisten aufgeführt aber im Bus gefunden worden, so wird dies durch ein gelbes Symbol deutlich gemacht. Der Zutrittsleser ist nicht initialisiert und seine LED leuchtet rot. Solange ein Leser initialisiert wird, ist das Verbindungssymbol rot. Alle in der Liste vorhandenen und initialisierten Zutrittsleser werden mit einem grünen Symbol kenntlich gemacht.



### 3.2.2.4. Inbetriebnahme-Modus für den Elektriker

Allgemeine Info:

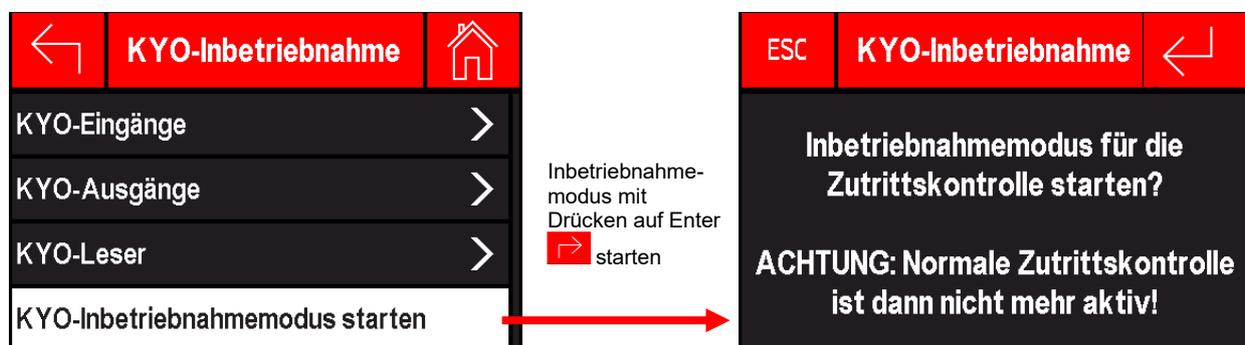
Der Inbetriebnahme-Modus dient dazu, die Installation zu prüfen.

Der Elektriker kann einen Ausweis ganz einfach zum System hinzufügen, um zum einen die Leser zu testen und zum anderen die Türöffnung (Relais) zu prüfen.

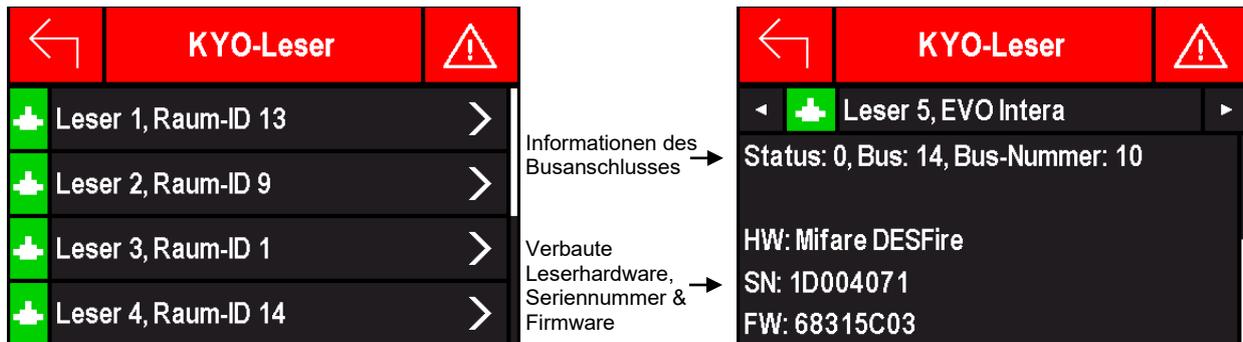
Um den Inbetriebnahme-Modus zu starten

Startet man nun den Inbetriebnahme Modus, sucht der KYO Cenloc alle sich im Bus befindlichen Zutrittsleser und initialisiert diese anschließend.

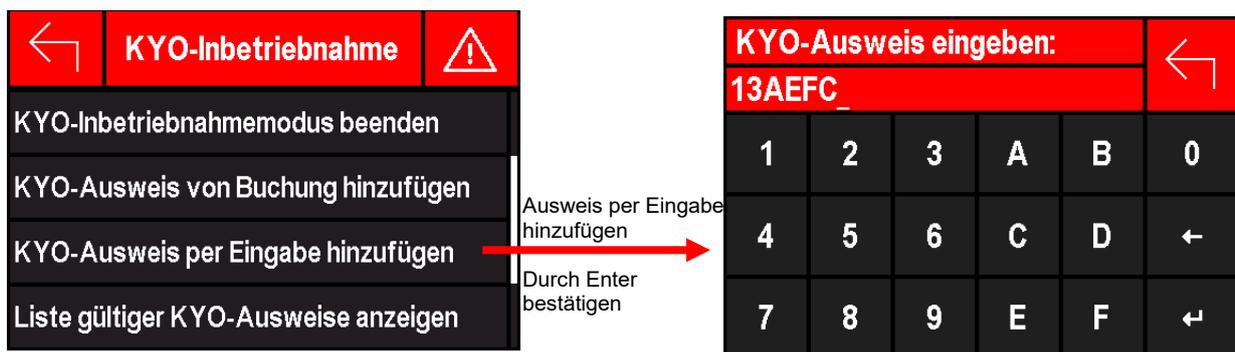
Der aktive Inbetriebnahme Modus wird durch das Achtung-Symbol deutlich gemacht.



Alle angeschlossenen Zutrittsleser werden unter dem Punkt KYO-Leser angezeigt und im Bus initialisiert, selbst wenn diese nicht in der Liste definiert sind. Jetzt können aus den dort angezeigten Informationen über die Zutrittsleser die Reader-Liste erstellt werden. Man erkennt hier auch, um welchen Leser-Typ mit welcher Bauform und Softwareversion es sich handelt.



Im Inbetriebnahme Modus können Transponder direkt eingelernt werden, die dann für die Zutrittskontrolle gültig sind. Dafür kann man den Transponderwert über eine Tastatureingabe eingeben oder man hält den Transponder vor einen der Zutrittsleser und fügt diesen über die Buchung dem Gerät hinzu.

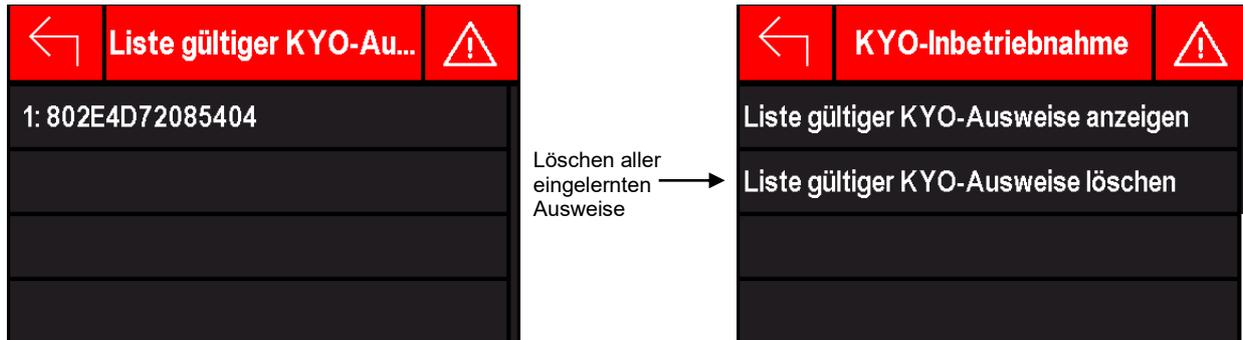


Nach Buchung an einem der Zutrittsleser werden der entsprechende Transponderwert und der Zeitpunkt der Buchung hinter dem Leser angezeigt. Durch Tippen auf das „“ auf der rechten Seite wird der Transponder gespeichert.

Nach erfolgreicher Speicherung des Transponders, wird dieser in grüner Schrift dargestellt. Wenn man den Transponder wieder zur Buchung nutzt, wird durch diesen der Zutritt gewährt.



Die Transponder, die per Buchung oder Tastatureingabe eingespeichert wurden, können im Menü in einer Liste angezeigt werden. Außerdem kann man die Liste der intern gespeicherten Transponder wieder löschen, um wieder neue Transponder anlegen zu können, falls die Liste voll ist (maximal 10 Ausweise möglich). Im Inbetriebnahmemodus werden die in der Identification-Liste angelegten Transponder ignoriert.

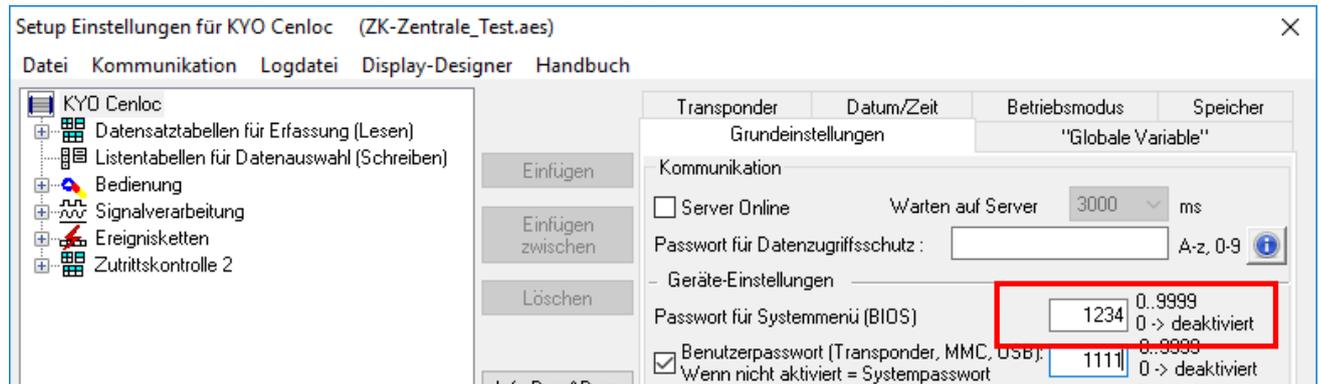


Durch Beenden des Inbetriebnahme Modus werden alle Leserinitialisierungen verworfen und nur noch Leser, die in den Zutrittslisten definiert sind, von dem KYO Cenloc in Betrieb genommen. Alle anderen Leser blinken dauerhaft weiß, diese müssen noch in die Reader-Liste hinzugefügt oder deren DIP-Schalterstellungen überprüft werden.

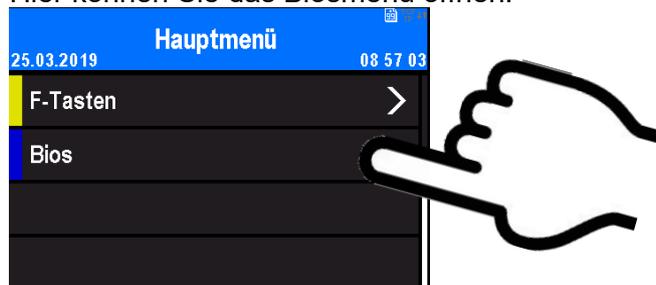


### 3.2.2.5. Aufbau Display Cenloc Bios-Menü

Ein Passwortschutz für das Biosmenü können Sie über das DatafoxStudioIV einrichten.



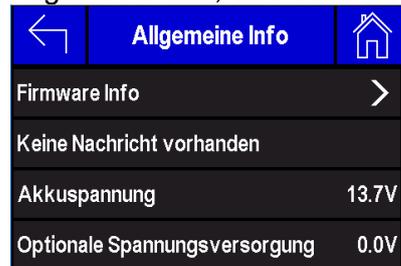
Hier können Sie das Biosmenü öffnen:



Die Erste Seite zeigt Ihnen:



Allgemeine Info, dies sollte selbsterklärend sein.

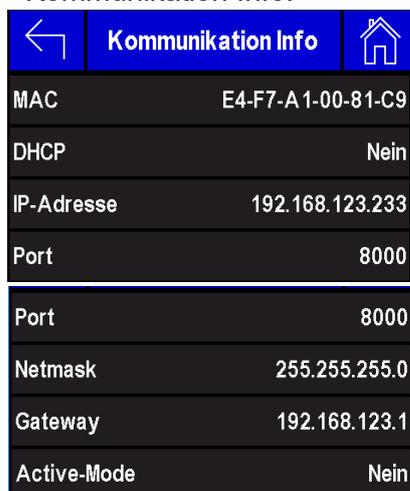


Benutzereinstellungen:



**Geräteneustart:**  
Hier kann das Gerät neu gestartet werden, Reboot!

Kommunikation Info.



**Kommunikation Info:**  
In diesem Menü können Sie keine Änderungen vornehmen!

Sollte das Gerät auf „DHCP“ stehen, können Sie die vom DHCP-Server zugewiesene IP einsehen.

### Benutzereinstellungen, Anzeige:

← Anzeige / Signallautst... 	
Displaybeleuchtung	100% >
Signallautstärke	1% >
Ausrichtung	180° >

#### Anzeige / Signallautstärke:

Hier können die Displayhelligkeit und die Signallautstärke des Buzzers angepasst werden.

Für den Fall, dass die Platinen Version des KYO Cenloc mal auf „Kopf“ montiert werden muss, können Sie die Anzeige des Display drehen.

### Systemmenü Bios

← Systemmenü Bios 	
Firmware Info	>
System Info	>
Kommunikation	>
Anzeige / Signallautstärke	>

#### Systemmenü Bios:

Firmware Info, Anzeige, Datum /Uhrzeit sind identisch zum Menü „Allgemeine Info“.

Kommunikation:  
Hier können IP, Port und andere Verbindungsparameter eingegeben werden.

#### nächste Seite:

Anzeige / Signallautstärke	>
Datum / Uhrzeit	>

### Kommunikation:

← Kommunikation 	
Schnittstelle	LAN >
Active Mode	nein
HTTP Mode	nein
LAN Parameter	>

Wählen Sie hier die Schnittstelle für die Hauptkommunikation aus.

Parameter für Active-Mode (Standard = nein)

Parameter für HTTP (Standard = nein)

Einstellung der TCP/IP Parameter (IP-Adresse)

### 3.3. Kommunikationsarten der V4 Geräte



**Achtung:**

Die Kommunikationsart des Gerätes ist abhängig von dessen Ausstattung.  
Hier sind alle Kommunikationsarten aufgeführt, welche in den Geräten möglich sind.



**Hinweis:**

Datafox-Geräte sind in der Lage, die Daten verschlüsselt zu übertragen.  
Mehr zu diesem Thema finden Sie im Handbuch „DatafoxStudioIV“.

**Die Umschaltung der Kommunikation kann erfolgen:**

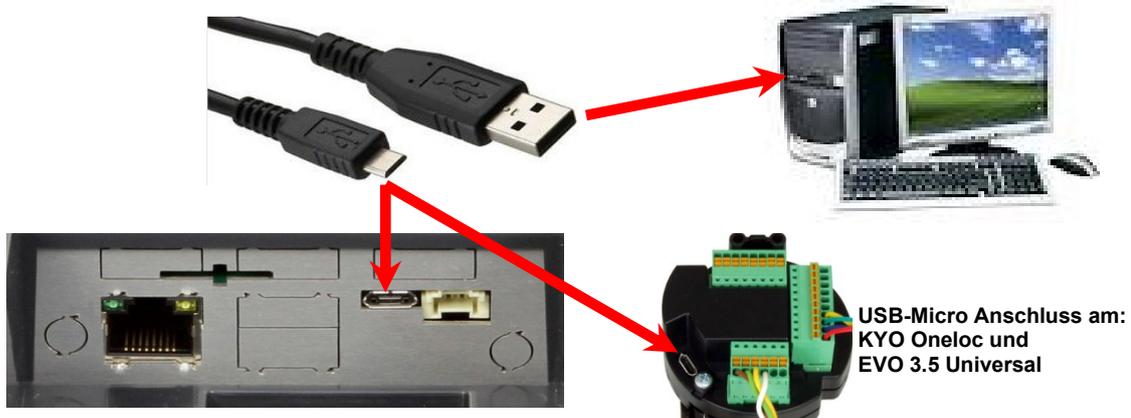
1. über Systemmenü Bios am Gerät
2. ab Firmware 04.02.04 im Setup mit der Feldfunktion „Kommunikation umschalten“. Mehr hierzu finden Sie im Handbuch [DatafoxStudioIV](#).

**Mögliche Kommunikationsarten sind:**

1. USB (an PC)
2. USB Host, Daten auf USB-Stick speichern GPRS Verbindung über das Mobilfunknetz

#### 3.3.1. Kommunikation der V4 Geräte über USB

Die Geräte der EVO-Line sind standardmäßig mit einer USB Schnittstelle ausgestattet. Die Geräte sind mit einem Micro-USB-B Anschluss ausgestattet. Dieser kann direkt mit dem PC verbunden werden.



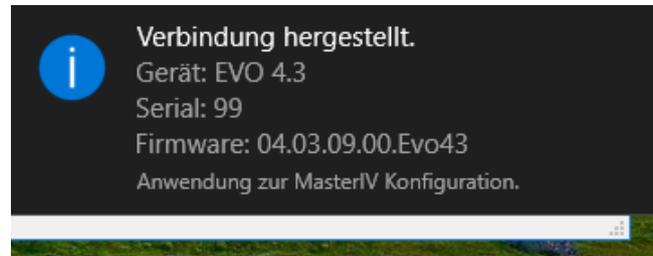
**Achtung:**

Für die Kommunikation mit den Evoline Terminals über USB ist zu beachten, dass es sich bei der USB-Schnittstelle des Terminals um einen Typ-B Anschluss handelt. Das heißt, dass das Terminal im Slave-Modus arbeitet und kann daher keine anderen USB-Geräte verwalten.

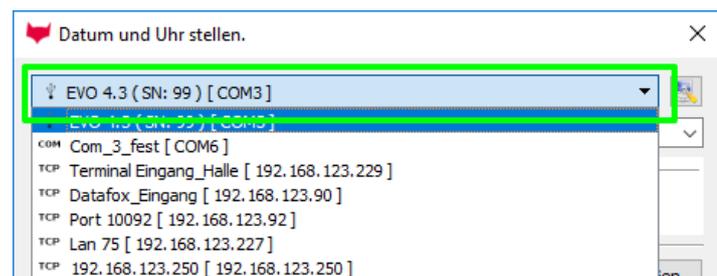
### 3.3.1.1. Automatische Erkennung über USB für V4 Terminals

Wird das Terminal über USB an einen PC angeschlossen, so erkennt dies das Terminal und stellt die Hauptkommunikation auf USB um.

Das DatafoxStudioIV erkennt das Gerät ebenfalls automatisch und meldet dies in der Taskleiste:



Das neu erkannte Gerät wird automatisch in die Verbindungsliste eingetragen.



Am Gerät selbst sehen Sie das Symbol für die Verbindung USB:



Somit fällt das zum Parametrieren der Geräte notwendige Aufrufen des Terminal→Systemmenü zum Umschalten der Kommunikation weg.

**Besonders praktikabel ist dies für die Boxengeräte.** Hier musste das Gerät über einen „Neustart“ und „Wechsel in das Biosmenü“ erzwungen werden.

Dies spart bei der Parametrierung der Geräte erheblich Zeit.

#### Hinweis:



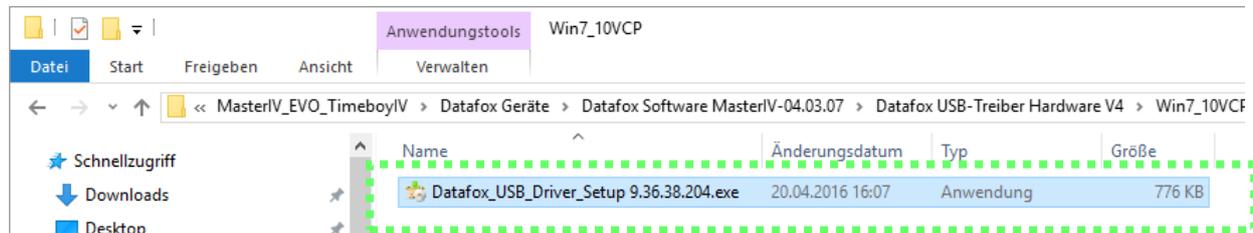
Wenn das Gerät per USB am PC angeschlossen ist, erfolgt keine Kommunikation über eine andere Schnittstelle wie Mobilfunk, IP etc.

Wird USB wieder entfernt, schaltet das Gerät selbstständig auf die vorher eingestellte Hauptkommunikation um.

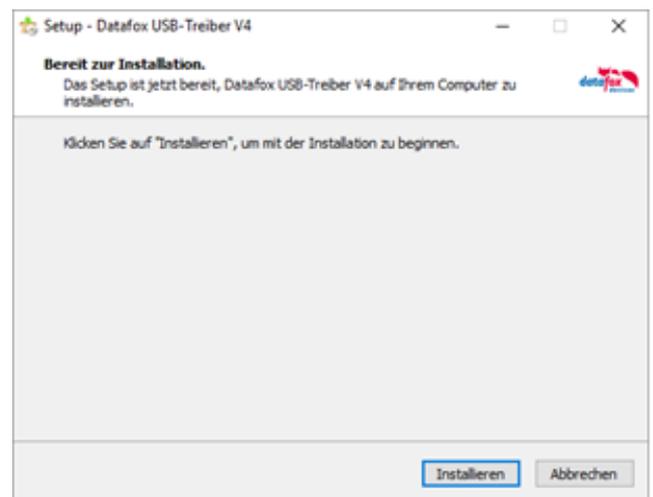
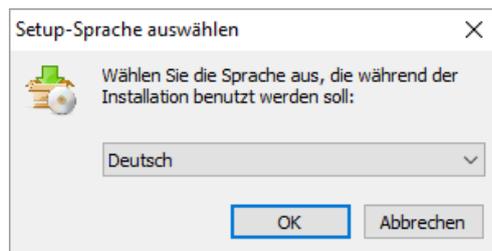
### 3.3.1.2. USB Treiberinstallation für Datafox Geräte HW V4

#### Installation für Windows 7, 8, 8.1 und 10.

Der USB Treiber ist ein kleiner Installer, der alle erforderlichen Einstellungen übernimmt. Führen Sie diese .exe einfach aus:



Folgen Sie den Anweisungen am Bildschirm:

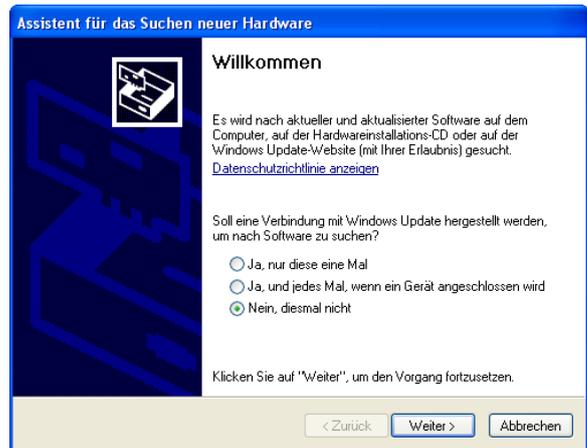


**!** **Achtung:**  
Es sind nur die zum Gerät mitgelieferten Treiber zu verwenden.

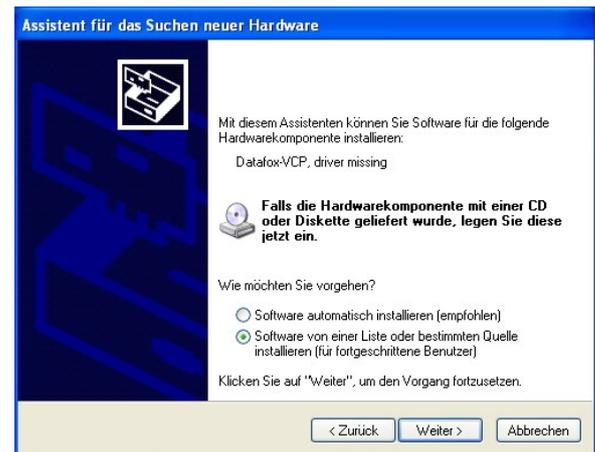
**👉 Hinweis:**  
Bei der Installation der Software „DatafoxStudioIV“ wird am Ende der gleiche Treiber automatisch mit installiert.

## Treiberinstallation USB mit Windows XP

Nachdem Sie den MasterIV an den PC angeschlossen haben, wird das Terminal als neues USB-Device erkannt und es beginnt die Installation der mitgelieferten USB-Treiber.



Nachdem Sie den MasterIV an den PC angeschlossen haben, wird das Terminal als neues USB-Device erkannt und es beginnt die Installation der mitgelieferten USB-Treiber.



## Treiberinstallation USB mit Windows XP

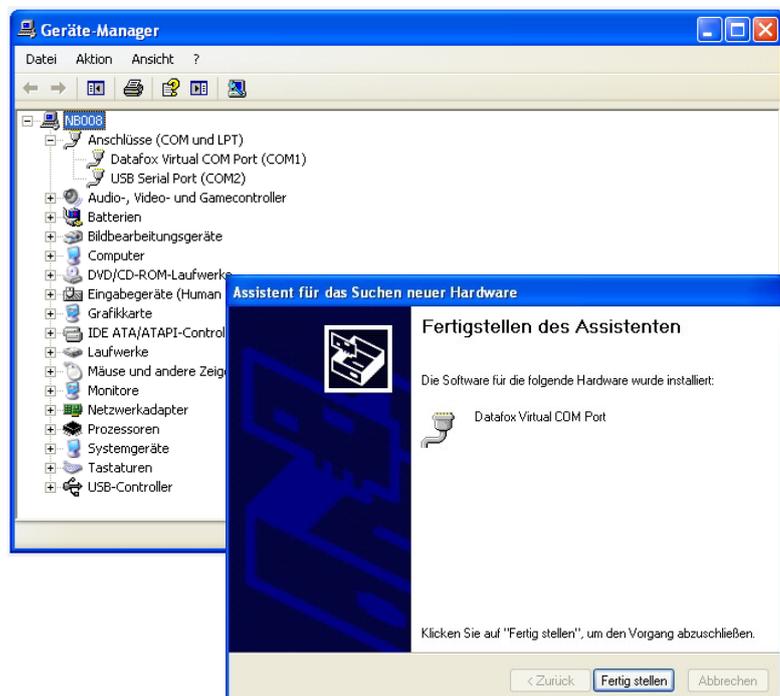
Wählen Sie den Ordner aus, in dem sich der mitgelieferte Treiber befindet.



Installation der Treiber für den virtuellen COM Port. Bei diesem Installationsschritt erhalten Sie die Meldung, dass der Treiber den Microsoft Logo-Test nicht bestanden hat. Hier müssen Sie auf „Installation fortsetzen“ klicken, um den Treiber nutzen zu können.



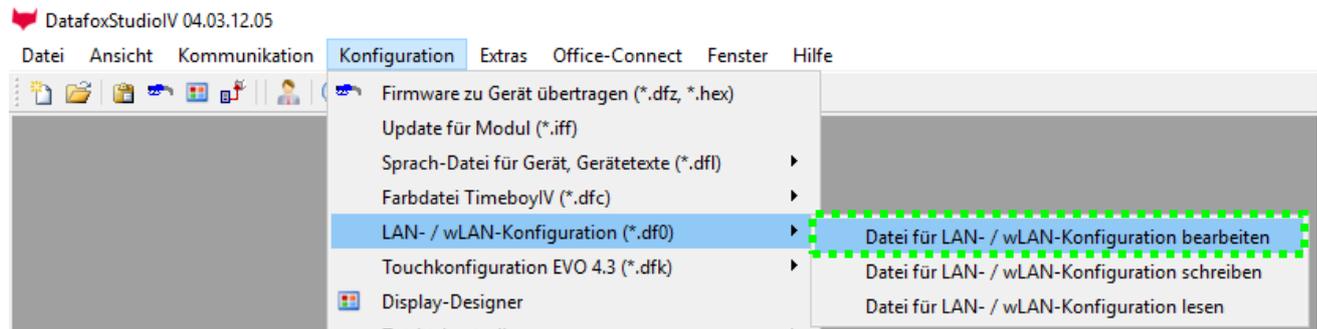
Im Geräte-Manager ist nun ein zusätzlicher COM Port vorhanden „Datafox Virtual COM Port“. Über diesen COM Port können Sie mit dem DatafoxStudioIV oder Ihrer eigenen Anwendung über die DFCOMDLL.dll eine Verbindung zum MasterIV Gerät aufbauen.





### 3.3.2. Kommunikation über TCP / IP

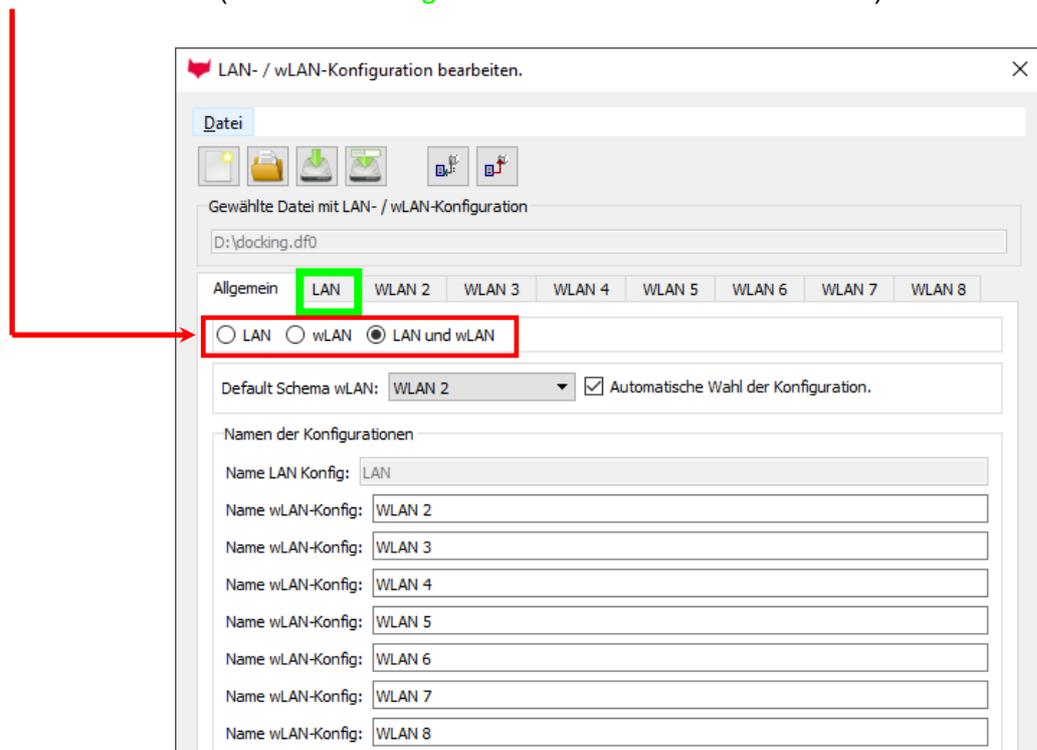
Die Einstellung der LAN / WLAN Parameter erfolgt über das DatafoxStudioIV unter dem Menüpunkt „Konfiguration“ → „LAN- / WLAN – Konfiguration (\*.df0)“.



Die LAN / WLAN Konfigurationen werden in einer Datei mit der Endung „\*.df0“ abgelegt. Hier haben Sie nun die Möglichkeit die Datei zu bearbeiten, in das Datafox-Gerät zu laden (hochladen) oder aus dem Gerät zu lesen (runterladen). Beim Lesen der WLAN Einstellung aus dem Gerät wird die aktuell angegebene Datei überschrieben.

In dem Register allgemein stellen als erstes ein mit welcher Hauptkommunikation das Gerät ausgestattet ist.

- Gerät mit LAN (Die erste Konfiguration ist für LAN Anschluss)
- Gerät mit WLAN
- Gerät mit LAN und WLAN (Die erste Konfiguration ist für den LAN Anschluss)



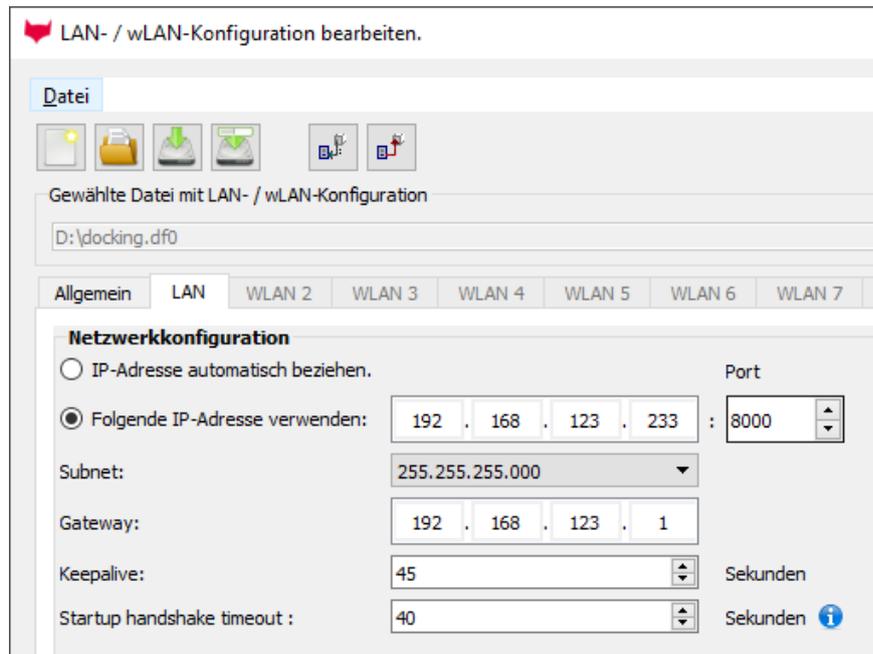
**Achtung:** Für TimeboyIV gilt, es darf nur die Einstellung wLan genutzt werden.

LAN 
  wLAN 
  LAN und wLAN 
     
  LAN 
  wLAN 
  LAN und wLAN

### 3.3.3. Kommunikation TCP / IP über LAN

Auf der Registerkarte „LAN“ können Sie die IP-Einstellungen vornehmen.

Geben Sie hier die gewünschte IP - Adresse, Subnet und wenn benötigt ein Gateway an.



LAN- / wLAN-Konfiguration bearbeiten.

Datei

Gewählte Datei mit LAN- / wLAN-Konfiguration

D:\docking.dfo

Allgemein LAN WLAN 2 WLAN 3 WLAN 4 WLAN 5 WLAN 6 WLAN 7

**Netzwerkkonfiguration**

IP-Adresse automatisch beziehen. Port

Folgende IP-Adresse verwenden: 192 . 168 . 123 . 233 : 8000

Subnet: 255.255.255.000

Gateway: 192 . 168 . 123 . 1

Keepalive: 45 Sekunden

Startup handshake timeout : 40 Sekunden i

Bei Geräten mit Display, kann die IP-Adresse auch direkt am Gerät eingegeben werden. Drücken Sie ESC und ENTER gleichzeitig um in das Bios-Menü des Geräte zu gelangen. Bei Geräten ohne Tastatur drücken Sie länger auf das Logo.

Mehr finden Sie im Kapitel „Bios-Menü“.

### 3.3.4. Kommunikation TCP / IP über WLAN

Allgemeine Info zu den verwendeten WLAN-Modulen.

Es gibt 2 Verschiedene WLAN-Module die in die Datafox-Geräten integriert worden.

- 1.) Redpine – seit dem Jahr 2013 in den Geräten verbaut.
- 2.) Texas Instruments TI-CC3135 – seit dem Jahr 2021.03 in den Geräten verbaut.

Grundsätzlich können Beide Module über das DatafoxStudioIV oder am Gerät selbst eingestellt werden.

Einziger Unterschied, der Module ist, dass unterschiedliche Standards unterstützt werden. Was jedes Modul im Einzelnen unterstützt, sehen Sie auf den nachfolgenden Seiten.

Welches Modul haben Sie oder wie finden Sie es heraus?

**Sie schauen mit dem DatafoxStudioIV über Konfiguration-> Gerätekonfiguration (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.
---------------	-------------------------	---	---	---

Oder

Standardmodul	M111_WLAN ESP32-C3 ML01			
---------------	-------------------------	--	--	--

oder

**Sie haben einen Lieferschein und schauen auf die Artikelnummer**

- 1.) Redpine: Art.Nr.: xxx112 (wLAN-Modul DF-WL01)
- 2.) Texas Instruments CC3135: Art.Nr.: xxx112 A (wLAN-Modul DF-WL02)
- 3.) M111\_WLAN ESP32-c3 ML01 Art.Nr.: xxx112 B (wLAN-Modul DF-WL03)

**Sie schauen im Bios-Menü des Gerätes:**

Unter: System Menu-> Systemmenü  
Bios-> Kommunikation  
Hier müssen Sie das Gerät auf „WLAN“  
als Hauptkommunikation einstellen.  
Unter den Einstellungen WLAN-Parameter haben Sie ein Info-Menü „Modul Informationen“.



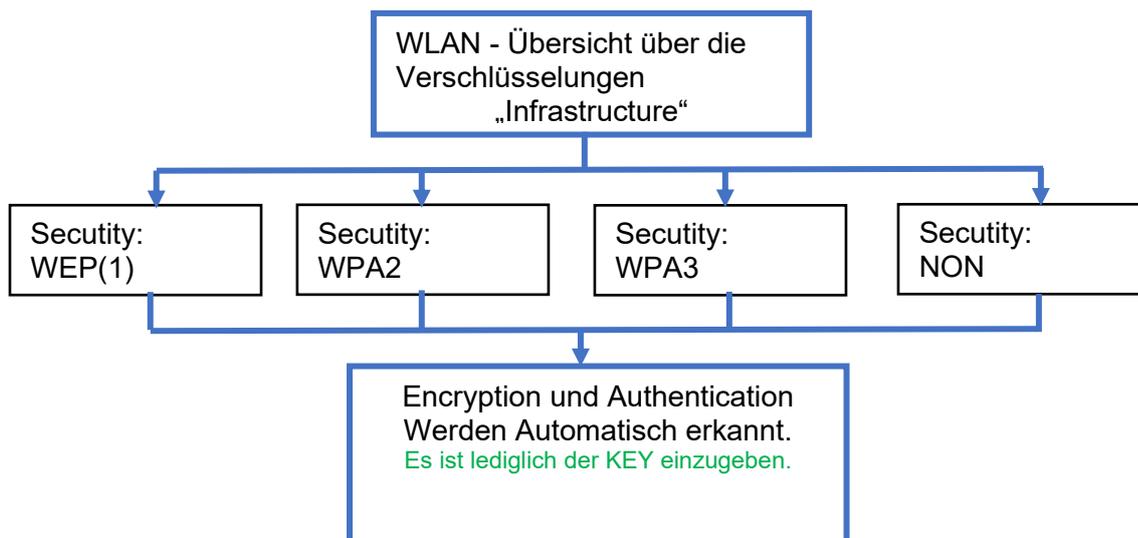
### 3.3.4.1. M111\_WLAN ESP32-c3 ML01 (wLAN-Modul DF-WL03)

Diese Übersicht zeigt Ihnen, welche WLAN Verfahren unterstützt werden.

Das WLAN 3 Modul erkennt automatisch die Verschlüsselung des AP. Daher muss nur der Security Parameter Eingestellt werden. Die Anderen Parameter (Encryption und Authentication) werden automatisch erkannt.

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

Unterstützt wird hier das 2.4Ghz Band.



#### **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.

### 3.3.4.2. Texas Instruments TI-CC3135 (Generation 2)

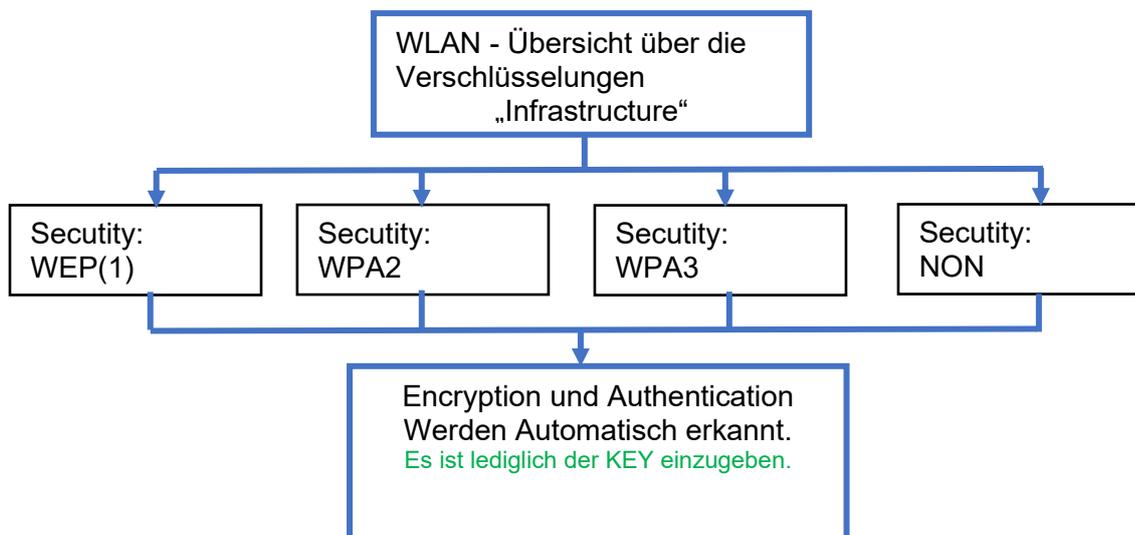
Diese Übersicht zeigt Ihnen, welche WLAN Verfahren unterstützt werden.

Das TI-CC3135 Modul erkennt automatisch die Verschlüsselung des AP. Daher muss nur der Security Parameter eingestellt werden. Die anderen Parameter (Encryption und Authentication) werden automatisch erkannt.

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

Im Fall, dass die Netze im 5Ghz und 2.4Ghz Band denselben Namen haben wird das Netz mit der besseren Empfangsqualität gewählt. Dies ist meistens das Netz im 2.4Ghz Band.

Unterstützt wird hier das 2.4Ghz und 5 Ghz Band.



#### 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.

**In Planung befindet sich die Unterstützung für WPA3 und WPA2 Enterprise.**

### 3.3.4.3. Redpine (Generation 1)

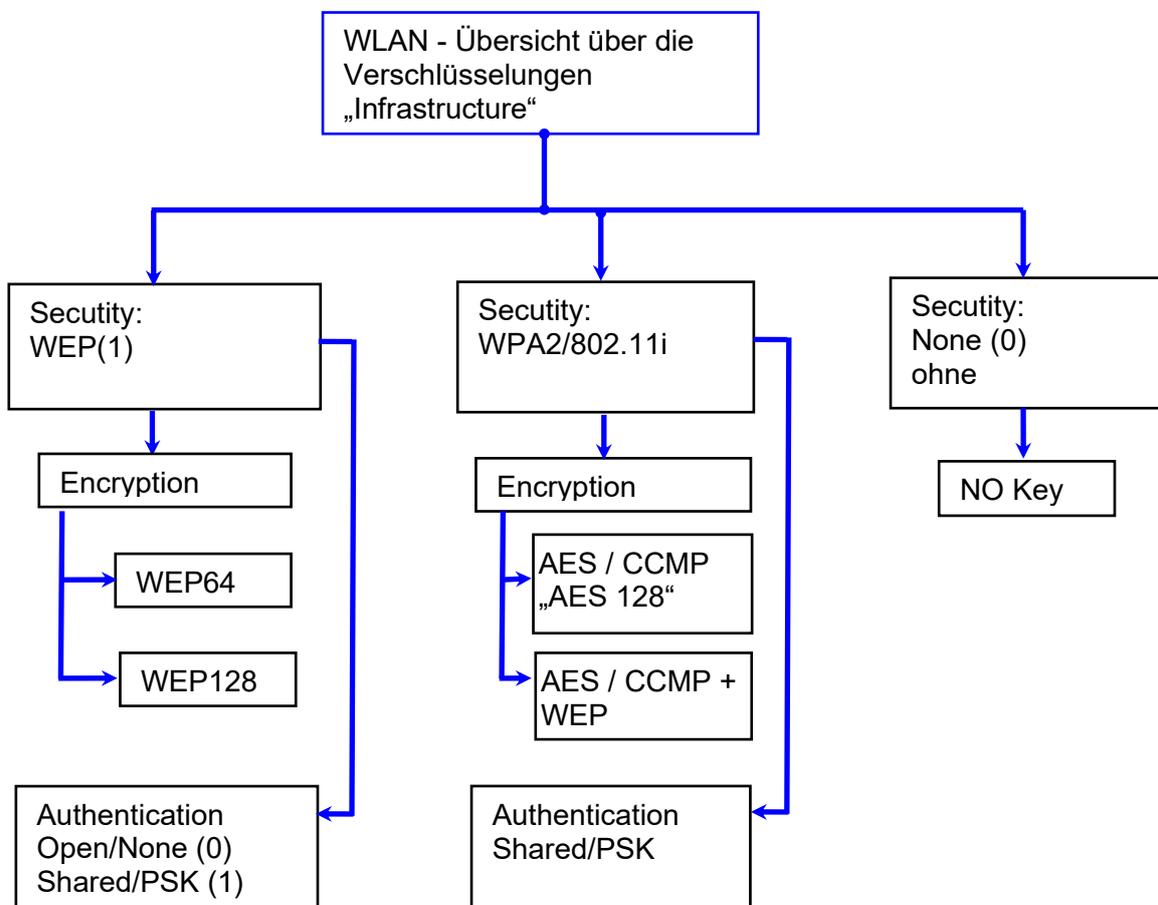
Diese Übersicht zeigt Ihnen, welche WLAN Verfahren unterstützt werden.

**Nicht** Unterstützt wird WPA (Vorgänger vom WPA2).

**Nicht** Unterstützt wird multiple-input multiple-output (MIMO)

**Nicht** Unterstützt werden 5 GHz Verbindungen und auch keine Mischbetrieb 2,4GHz / 5 GHz.

**Nicht** Unterstützt wird die Authentifizierung via WPA2 Enterprise nach IEEE 802.1x



#### 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.



#### Achtung:

[multiple-input multiple-output](https://en.wikipedia.org/wiki/Single-input_single-output_system) (MIMO) wird nicht unterstützt. Wenn Sie den AP von b/g/n zu b/g umschalten, wird automatisch nur SISO verwendet.  
[https://en.wikipedia.org/wiki/Single-input\\_single-output\\_system](https://en.wikipedia.org/wiki/Single-input_single-output_system)

Bei der Einstellung der Verschlüsselung AES oder WEP wird immer nur eine Art verwendet. Die Einstellung AES+WEP bedeutet bei manchen AP's, dass erst eine AES Verschlüsselung durchgeführt wird und danach noch zusätzlich mit WEP verschlüsselt wird. Stellen Sie für diesen Fall nur AES ein.

### 3.3.4.4. Einstellen der WLAN Parameter

Wählen Sie hier die Konfiguration bzw. den Standort, für den Sie die WLAN Parameter einstellen möchten.

Geben Sie hier die IP-Adresse für das Gerät ein. Diese muss für jeden Standort gleich sein.

Hier können alle Einstellungen vorgenommen werden, die für ein AP notwendig sind.

Ist ein Key hinterlegt, so wird Ihnen dies so angezeigt

Setzen Sie diesen Haken, so erhöht sich die Akkulaufzeit deutlich, sofern ein Betrieb mit Akku beim Gerät vorgesehen ist. **Wichtig bei TimeboyIV!**

The screenshot shows the 'LAN- / wLAN-Konfiguration bearbeiten' window. It includes sections for 'Datei', 'Netzwerkkonfiguration', 'wLAN-Konfiguration', 'wLAN-Netzwerksicherheit', and 'Optionen'. Annotations include red arrows pointing to the location dropdown (highlighted with a red dashed box), the IP address fields, and the key field. A blue arrow points to the 'Power Save aktivieren' checkbox in the 'Optionen' section, which is also highlighted with a green dotted box.

Ein Scan (Suche) nach APs, wird nach einem Verbindungsabbriss erst nach dieser eingestellten Zeit durchgeführt. Beachten Sie dazu die nachfolgende Achtung Box!

**Achtung:**  
 Eine Suche nach einem neuen AP, benötigt sehr viel Energie und entleert den Akku dadurch. Vermeiden Sie eine dauernde Suche nach einem AP, wenn das Gerät im Grenzbereich arbeitet, in dem Sie die Pause zwischen den Scans nach neuen APs großzügig wählen (80-120s).  
 An den meisten AP gibt es die Möglichkeit das „Beacon Interval“ einzustellen. Je höher dies eingestellt ist, umso weniger Strom benötigt der TimeboyIV. Empfehlung: Bacon Interval >300ms.

Die gesamte Datei, mit allen Einstellungen wird in das Gerät übertragen. Verfügt das Gerät über ein Display, kann im Bios-Menü → Kommunikation → WLAN kann der Standort gewählt werden. Je Standort wird eine eigene Konfiguration für die WLAN – Anbindung hinterlegt. Der User hat somit keinen Einblick auf die Einwahlparameter an den verschiedenen Standorten.

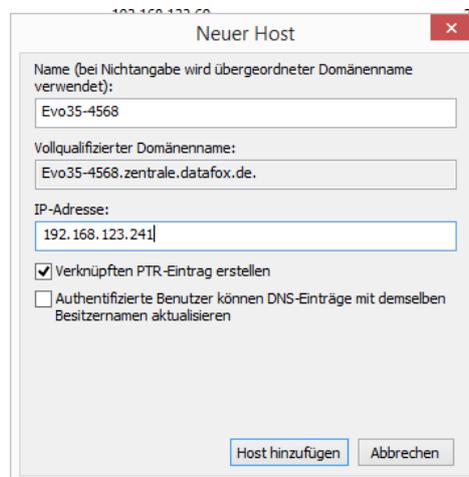
**Hinweis:**  
 Bei automatischer Wahl der Konfiguration / Standort, wird immer zuerst versucht, die Verbindung mit dem Default-Schema aufzubauen.

### 3.3.4.5. Verbindung der Terminals via TCP/IP DNS / DHCP

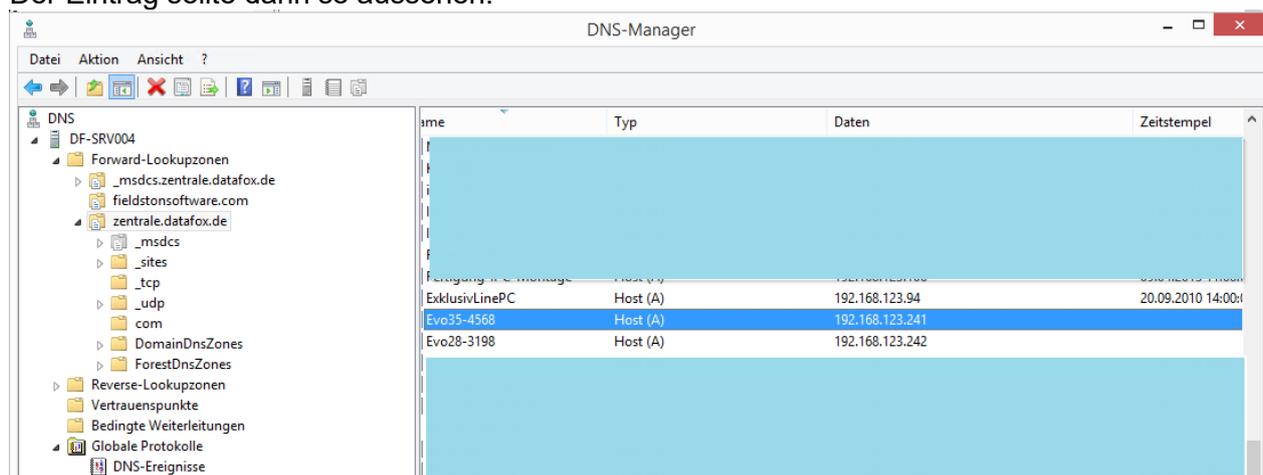
Um ein Datafox EVO-Gerät über den Hostname zu erreichen sind zunächst einige Einstellungen im DNS-Server notwendig. (In unserem Beispiel Fall Windows-Server 2012)

Es muss ein neuer Host (A)-Wert erstellt werden:

Abkürzung	Beschreibung
Name	Der Name des Gerätes Er setzt sich zusammen aus der Gerätebezeichnung und der Seriennummer „GerätXX-Seriennummer“ Beispiel: „Evo28-1652“ „EVO43-8552“
Vollqualifizierter Domänenname	Dies ist der Hostname der später eingegeben werden muss.
IP-Adresse	Hier muss die IP des Gerätes eingegeben werden
Verknüpfter PTR-Eintrag erstellen	Es muss ein verknüpfter PTR-Eintrag erstellt werden. Dazu einfach diesen Haken setzen.

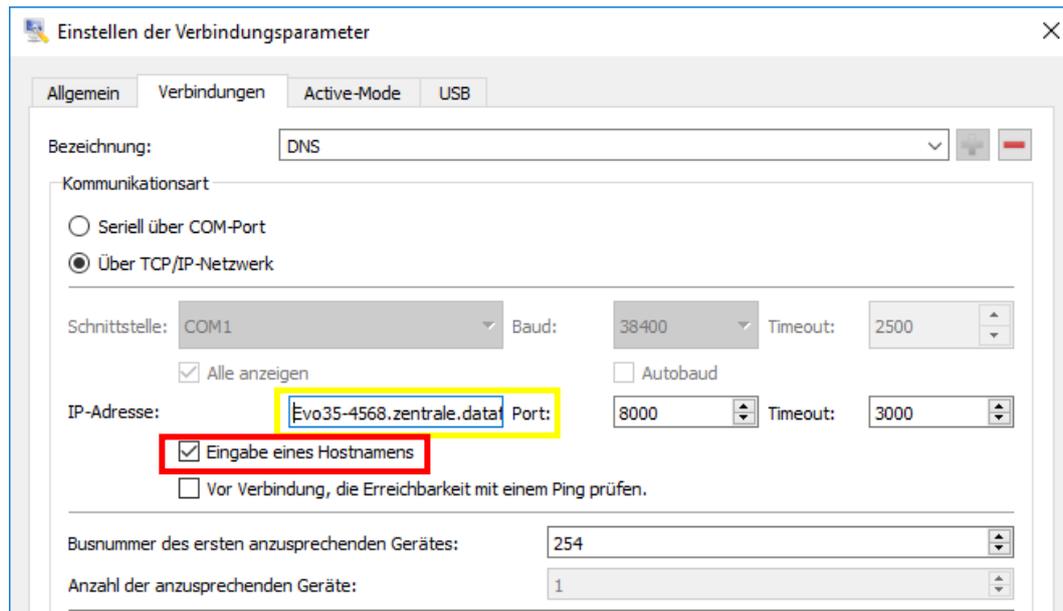


Der Eintrag sollte dann so aussehen:



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	20.09.2010 14:00:00
Evo28-3198	Host (A)	192.168.123.242	20.09.2010 14:00:00

## Einstellung im Datafox Studio:



Hier wird der Hostname  
eingegeben.

Vor der Eingabe muss  
dieser Haken gesetzt wer-  
den.

## DHCP- Eintrag für Datafox Geräte

Steht ein Gerät auf DHCP, kann die IP Adresse und der Eintrag im DHCP Server wie folgt aussehen.

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

Der Eintrag setzt sich wie folgt zusammen:

Gerät	Seriennummer	Domain	DHCP- Eintrag
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

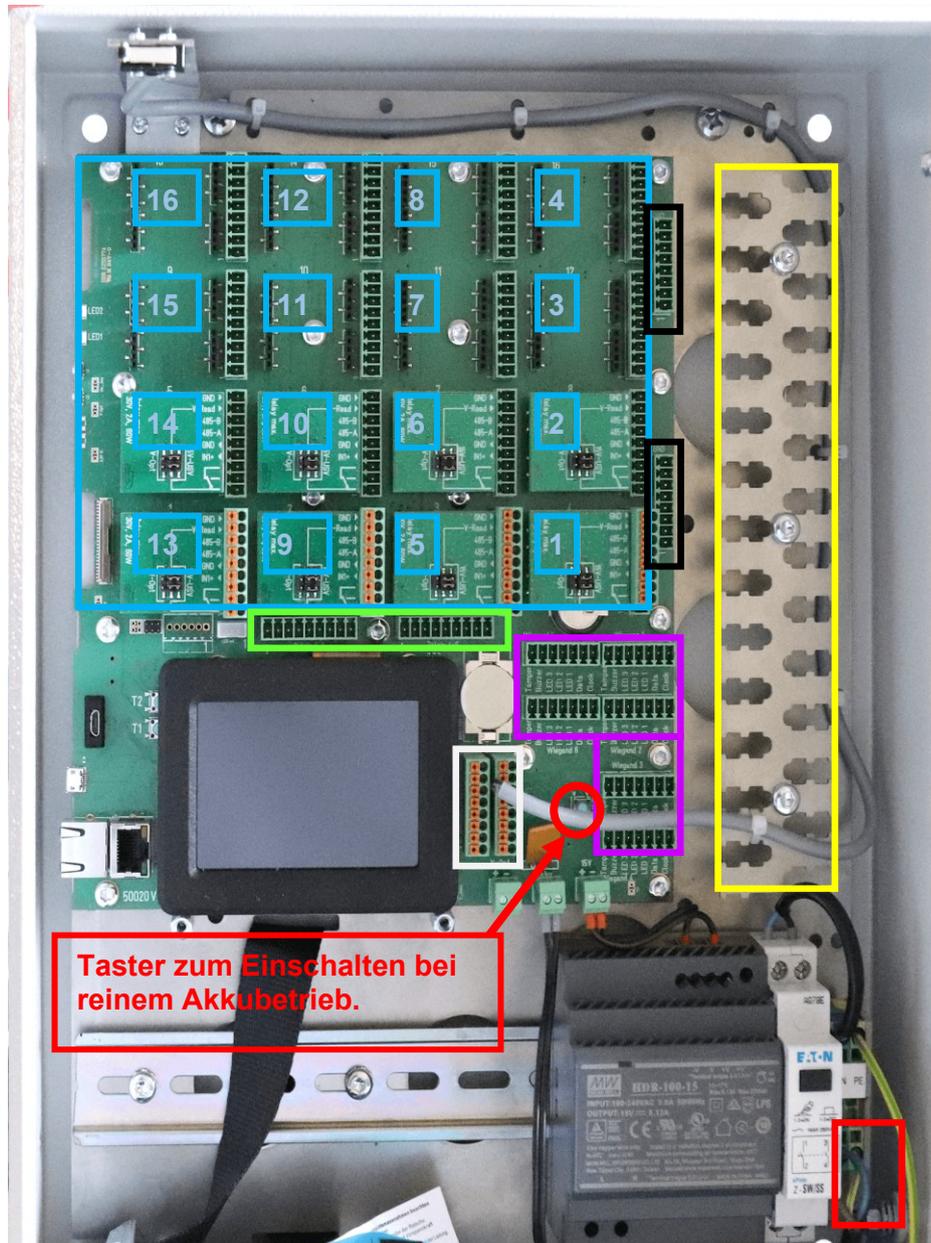


### 3.4. Anschluss KYO-Cenloc

#### Übersicht der Anschlüsse:

Steckplätze für Erweiterungsmodule.  
Wenn eine Erweiterung erfolgt, sollten die Module immer aufsteigend bestückt werden.  
Modulplatz 1, 2, 3, usw.

Stecker für den Anschluss GND  
Ground / Masse



Befestigungsleiste zur Zugentlastung der Anschlussleitungen.  
Hier können die Leitungen mittels Kabelbinder befestigt und deren Schirmungen aufgelegt werden.

Anschluss für digitale Ausgänge (6x Relais).

Anschluss für digitale Eingänge.  
Links digi. In 17-20  
Rechts digi. In 21-24

Anschluss externer Zutrittsleser mit Wiegand-Interface.

Anschluss 230 V L/N/PE  
L-Außenleiter  
N-Neutralleiter  
PE-Schutzleiter

**! Die Anlage darf nur mit angeschlossenem Schutzleiter in Betrieb genommen werden.**

**Taster zum Einschalten bei reinem Akkubetrieb.**

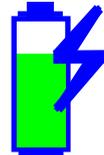
### 3.4.1. Spannungsversorgung des KYO-Cenloc

#### 3.4.1.1. Spannungsversorgung 230V Netzanschluss

Die Versorgungsspannung geschieht mittels eines Netzteils 15V DC / 92 W.  
Über dieses Netzteil wird die Zentrale selbst versorgt, optional die angeschlossenen Leser versorgt und der Akku geladen.

Das Laden des Akkus wird anhand des Batterieladesymboles kenntlich gemacht.

**! Nur bei Betrieb mit Netzspannung ist die volle Funktionalität gegeben.**



#### Das Netzteil technische Daten:



##### ■ Features

- Ultra slim design with 70mm(4SU) width
- Universal input 85~264VAC(277VAC available)
- No load power consumption<0.3W
- Isolation class II
- Pass LPS (Limited power source) for Blank type
- DC output voltage adjustable
- Protections : Short circuit / Overload / Over voltage
- Cooling by free air convection (working temperature:-30~+70°C)
- DIN rail TS-35/7.5 or 15 mountable
- LED indicator for power on
- 3 years warranty

##### ■ Description

HDR-100 is one economical ultra slim 100W DIN rail power supply series, adapt to be installed on TS-35/7.5 or TS-35/15 mounting rails. The body is designed 70mm(4SU) in width, which allows space saving inside the cabinets. The entire series adopts the full range AC input from 85VAC to 264VAC(277VAC also available) and conforms to EN61000-3-2, the norm the European Union regulates for harmonic current. HDR-100 is designed with plastic housing that it can effectively prevent user from electric hazards. With working efficiency up to 91%, the entire series can operate at the ambient temperature between -30°C and 70°C under air convection. It is equipped with constant current mode for over-load protection, fitting various inductive or capacitive applications. The complete protection functions and relevant certificates for home automations and industrial control apparatus (IEC60950-1, UL508, UL60950-1, EN61558-2-16) make HDR-100 a very competitive power supply solution for household and industrial applications.

##### ■ Applications

- Household control system
- Building automation
- Industrial control system
- Factory automation
- Electro-mechanical apparatus

#### 3.4.1.2. Spannungsversorgung über POE

Wird beim Cenloc nicht angeboten!

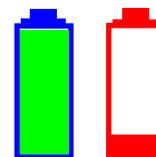
### 3.4.1.3. Spannungsversorgung über den internen Akku

Der Akku dient zur Überbrückung bei einem Stromausfall. Die Überbrückungszeit ist von der Geräteausrüstung abhängig und kann folgendermaßen berechnet werden:

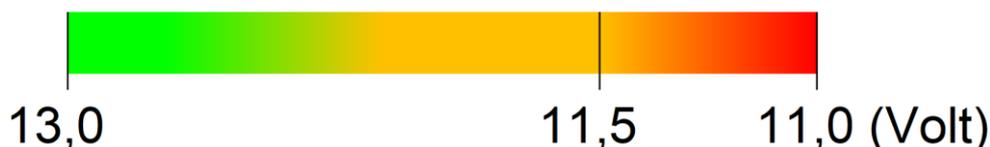
$$\text{Anzahl Stunden} = \text{Akkukapazität} / \text{Stromaufnahme des Gerätes (in Ampere)}$$

Der verwendete Akku verfügt über eine Kapazität von 7,2Ah, wenn sich dieser in neuwertigem Zustand befindet und voll geladen ist.

Je nach Ladezustand des Akkus, wird das Batteriesymbol mit einem Balken ausgefüllt.



Die Ladezustände des Akkus stellen sich folgendermaßen dar:



Spannungsbereich	Zustand
Von 13,0 Volt bis 11,5 Volt	Akkuspannung in Ordnung.
Von 11,5 Volt bis 11,0 Volt	Geringe Akkuspannung (das Batteriesymbol fängt an zu blinken).
Unter 11,0 Volt	Die ZK-Zentrale schaltet sich aus.

#### Achtung:



Wenn die Akkuspannung bei reinem Akkubetrieb unter 11,0 Volt sinkt schaltet sich die ZK-Zentrale selbstständig aus. Durch Anschließen der Netzspannung oder eines vollgeladenen Akkus, kann die ZK-Zentrale wieder gestartet werden. Falls versucht wird mit einem leeren Akku zu starten, schaltet sich die ZK-Zentrale nach dem Start selbstständig wieder aus.

### 3.4.1.4. Ausschalten des Gerätes und Wechsel des Akkus

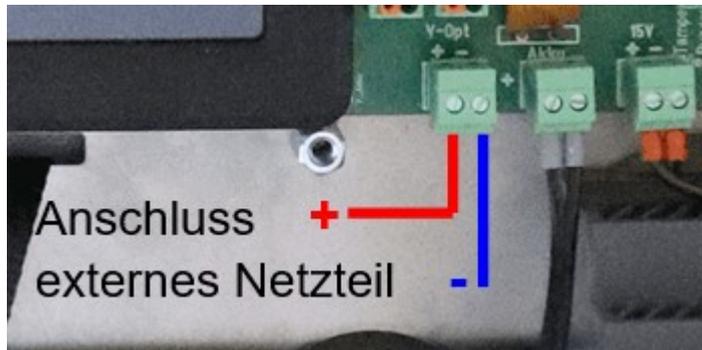
Wenn der Akku getauscht oder das Gerät aufgrund eines Transportes ausgeschaltet werden soll, gibt es die Möglichkeit das Gerät bei reinem Akkubetrieb über einen Menüeintrag im BIOS-Menü auszuschalten. Unter den Benutzereinstellungen taucht nur bei Akkubetrieb der Menüpunkt „Gerät parken“ auf. Nach dessen Betätigung schaltet sich das Gerät aus und der Akku kann abgezogen werden.

Wenn das Gerät ausgeschaltet ist, schaltet es sich beim Anlegen der Netzspannung wieder ein. Bei reinem Akkubetrieb kann das Gerät durch Drücken des Tasters (Siehe Bild) von drei Sekunden wieder eingeschaltet werden.

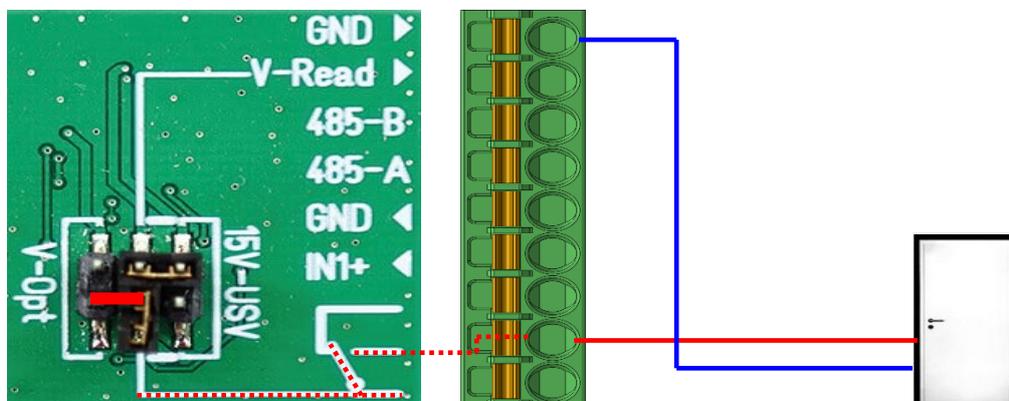
### 3.4.1.5. Spannungsversorgung über externe Spannungsquelle (DC)

Der Datafox KYO Cenloc kann alternativ auch mit einer externen Spannungsquelle versorgt werden. Diese wird mit Hilfe einer 2-poligen Schraubklemme - V-Opt - im Anschlussbereich der Platine aufgelegt und das zugehörige Netzteil auf der Hutschiene montiert werden.

Die Spannung V-Opt (Optional) wird auf der Hauptplatine auf alle Erweiterungsmodule zum Anschluss der Zutrittsleser durchgeschliffen und kann über die Jumperleiste des Modules für die Zutrittsleser abgegriffen werden.

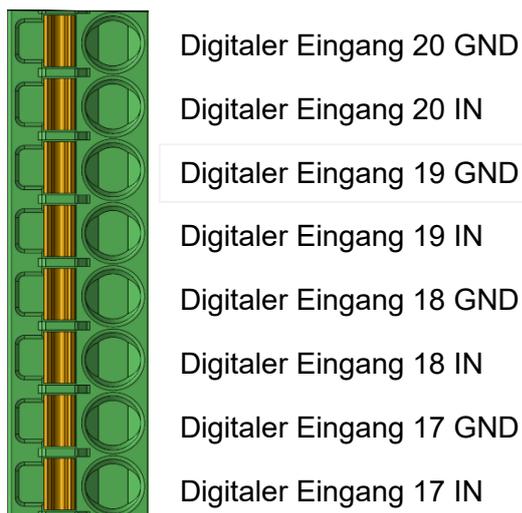


Beispiel Stromführung auf dem Erweiterungsmodul:

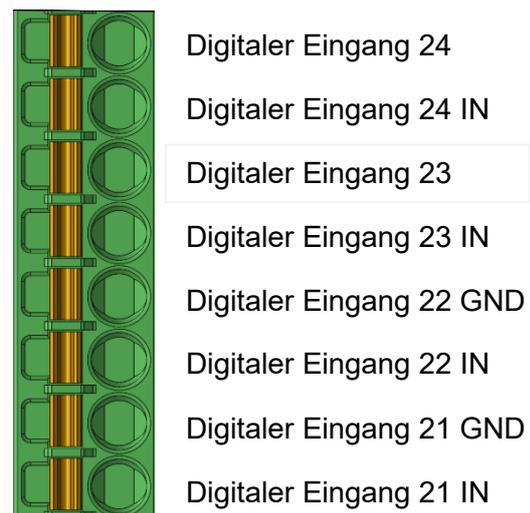


### 3.4.1.6. Anschluss der digitalen Eingänge

Stecker links:

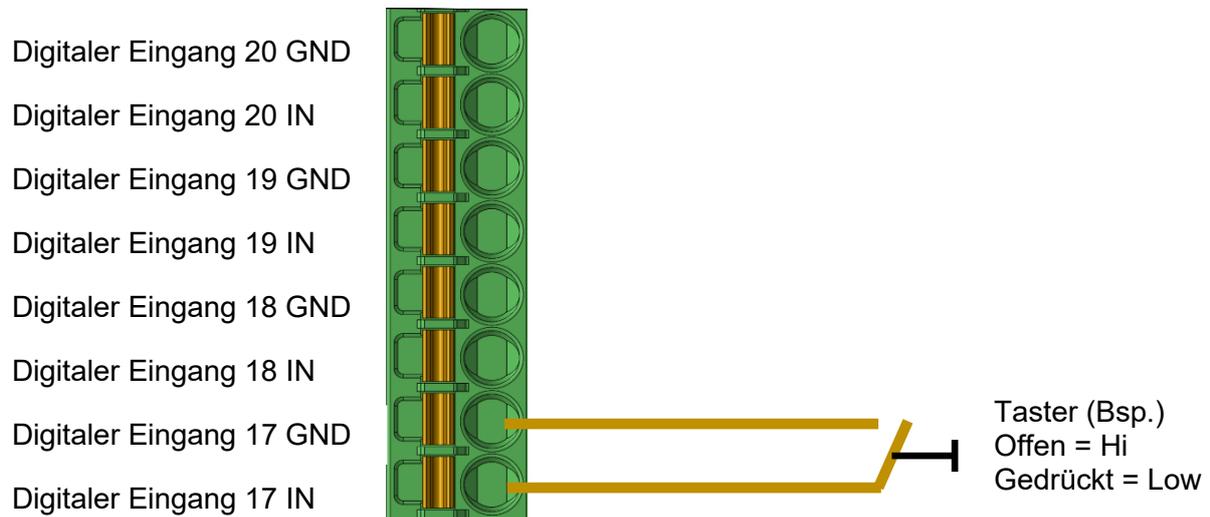


Stecker rechts:

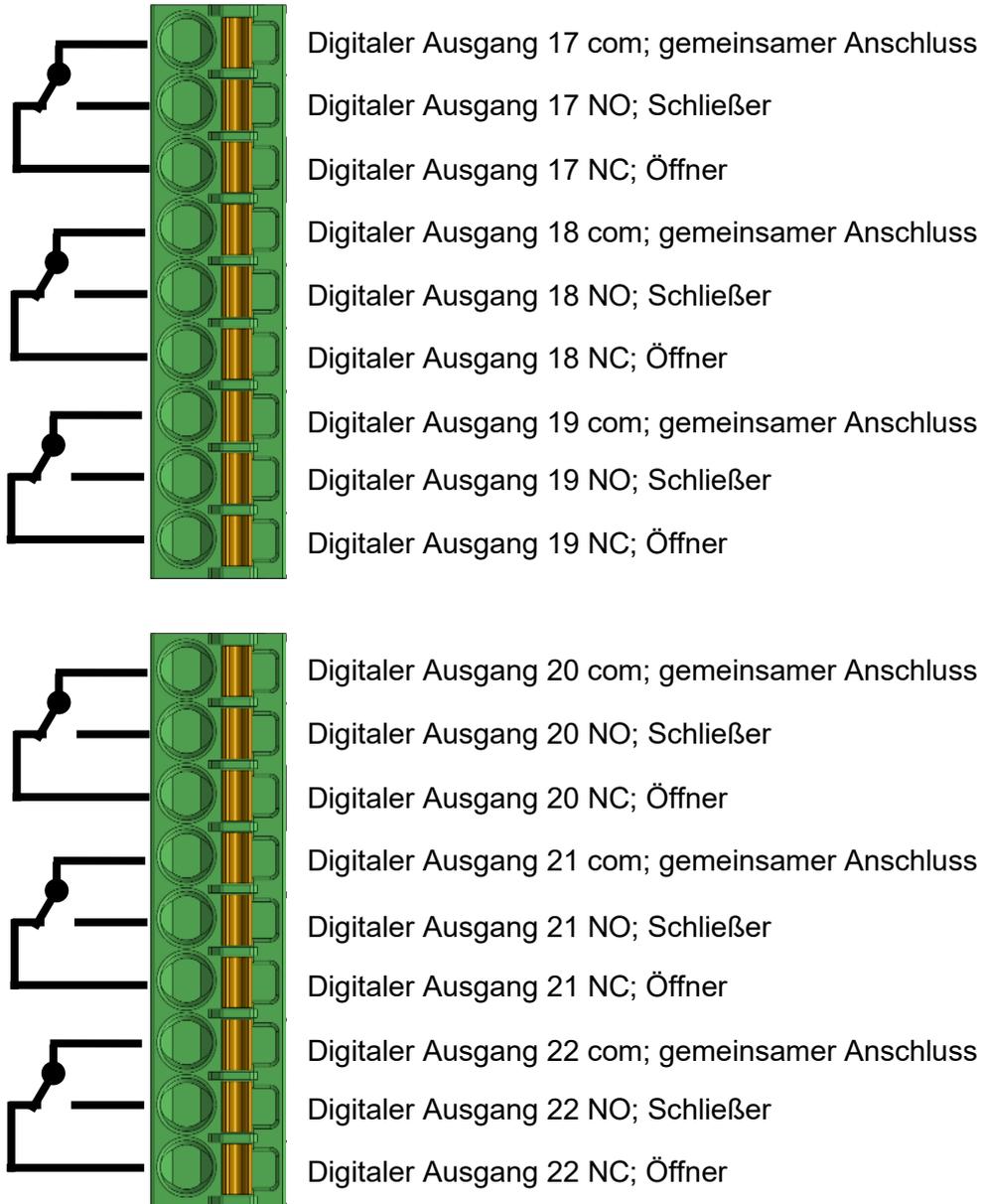


### Schaltbeispiel:

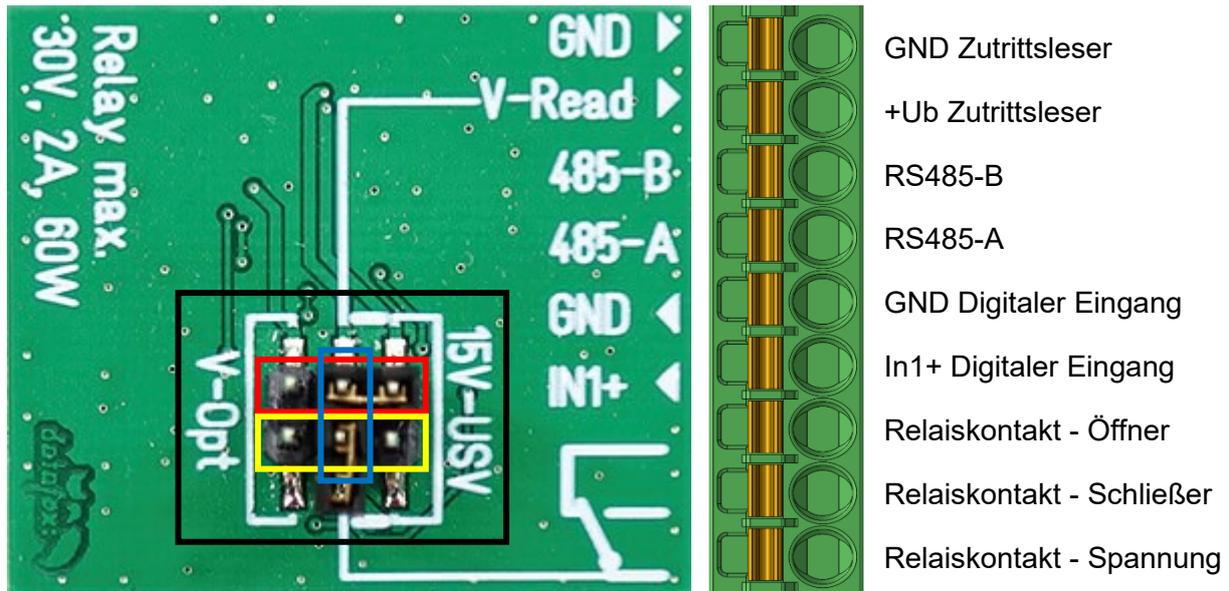
Der jeweilige Anschluss „IN“ liegt intern über einen Pullup-Widerstand auf Hi-Signal.  
 Durch Brücken mit dem jeweiligen daneben liegenden Masseanschluss wird das Signal auf dem Eingang „Low“.



### 3.4.2. Anschluss der digitalen Ausgänge auf der Hauptplatine



### 3.4.3. Beschreibung der Erweiterungs-Module



Jumperleiste des Erweiterungsmoduls.

Hier können, jeweils horizontal, Jumperbrücken gesteckt werden. Aktuell befinden sich die Jumper im Auslieferungszustand, so dass die Zutrittsleser mit dem integrierten Netzteil bzw. der USV versorgt werden und am Relais keine Spannung anliegt, um Kurzschlüsse abhängig des Anwendungsfalls zu vermeiden. Die verschiedenen Jumperstellungen erfüllen folgende Aufgaben.

**! Pro Modul können mit dem integrierten Netzteil 350mA Strom abgenommen werden. Dies entspricht einem EVO Intera und einem EVO Agera-Zutrittsleser an einem Busstrang.**

Die obere Jumperleiste dient zur Spannungsversorgung der angeschlossenen Zutrittsleser. Setzt man den Jumper auf die linke Position, so werden die angeschlossenen Leser mit einem externen Netzteil versorgt. Dies ist der Fall, wenn die Zutrittsleser mit mehr als 15V Versorgungsspannung arbeiten.

Ist der Jumper, wie in der Abbildung zu sehen, auf die rechte Position gesteckt, werden die Zutrittsleser mit dem im KYO Cenloc integrierten Netzteil bzw. dem USV-Akku versorgt.

Die zweite Jumperleiste gibt die anliegende Spannung an das Relais weiter. Jumper auf der linken Position bedeutet, dass die Spannung des externen Netzteils am gemeinsamen Relaiskontakt anliegt und entsprechend geschaltet werden kann. Setzt man den Jumper auf die rechte Position so liegt am Relais die Spannung des integrierten Netzteils bzw. des USV-Akkus an.

Für Jumperstellung drei besteht die Möglichkeit, die Schaltspannung des Relais direkt als Versorgungsspannung für die Zutrittsleser durchzuschalten.

**! Hierbei maximale Schaltleistung des Relais beachten.**



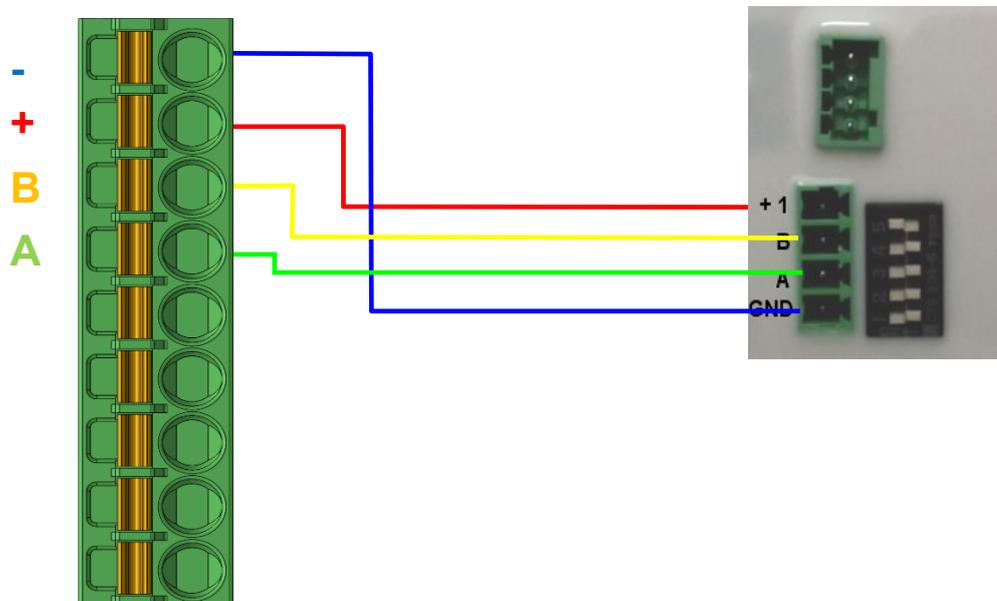
#### Achtung:

Die Steckmodule dürfen nur im ausgeschalteten Zustand gesteckt oder gezogen werden. Erst nach einem Neustart werden neue Module erkannt.

### 3.4.3.1. Anschluss eines Zutrittslesers an ein Erweiterungs-Modul

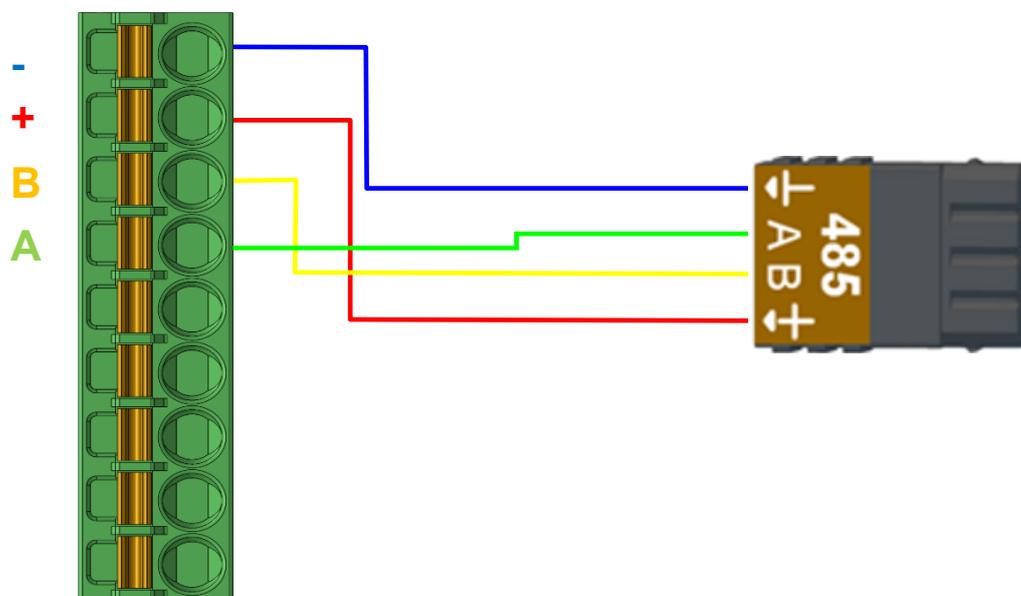
#### Verdrahtungsplan für einen EVO Intera

(hierbei gilt der gleiche Aufbau pro ZK-Strang bzw. ZM / Bus-ID)



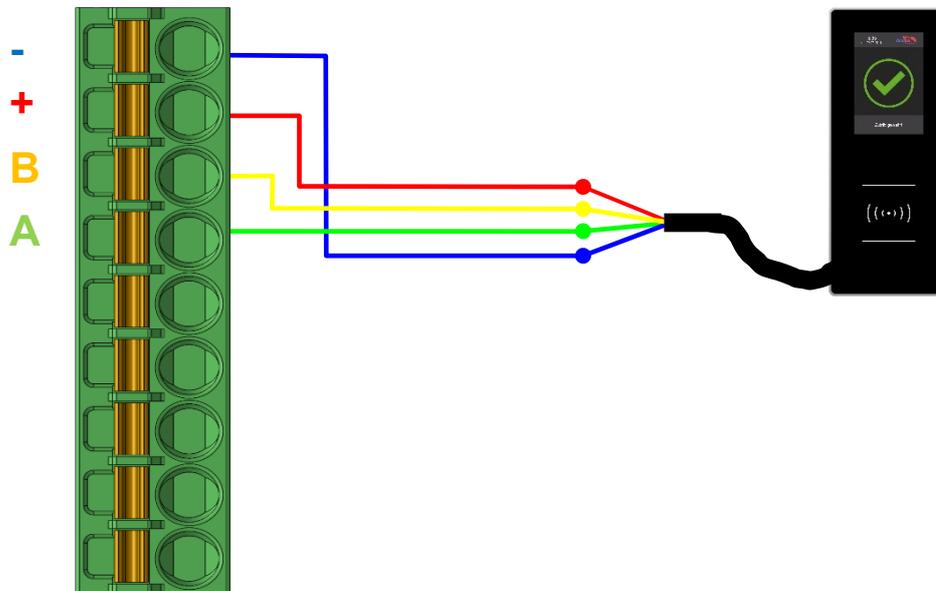
#### Verdrahtungsplan für einen EVO Intera II

(hierbei gilt der gleiche Aufbau pro ZK-Strang bzw. ZM / Bus-ID)



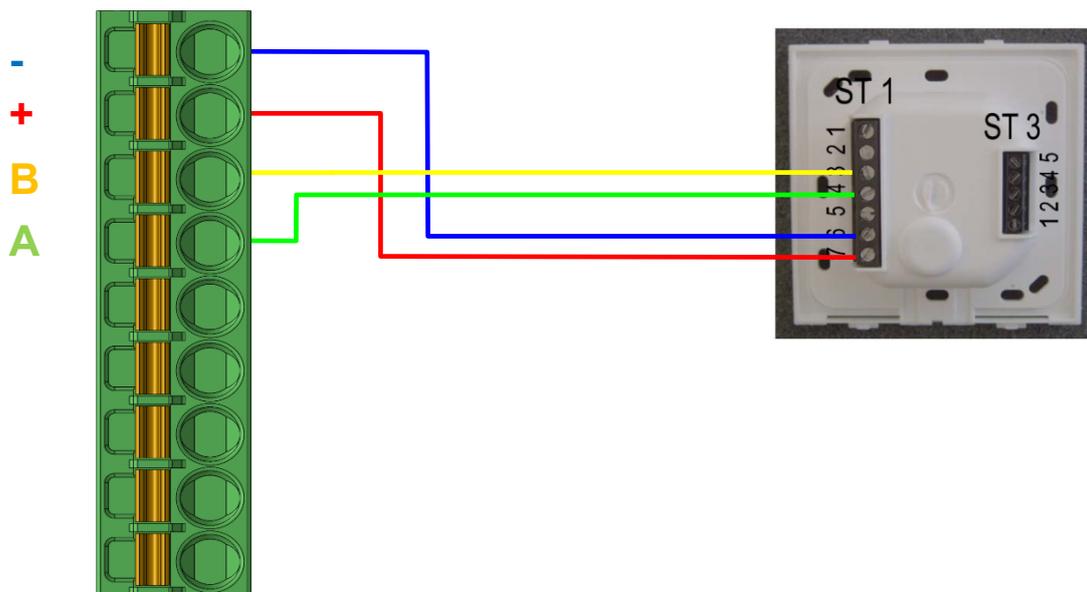
### Verdrahtungsplan für einen EVO Agera

(hierbei gilt der gleiche Aufbau pro ZK-Strang bzw. ZM / Bus-ID)

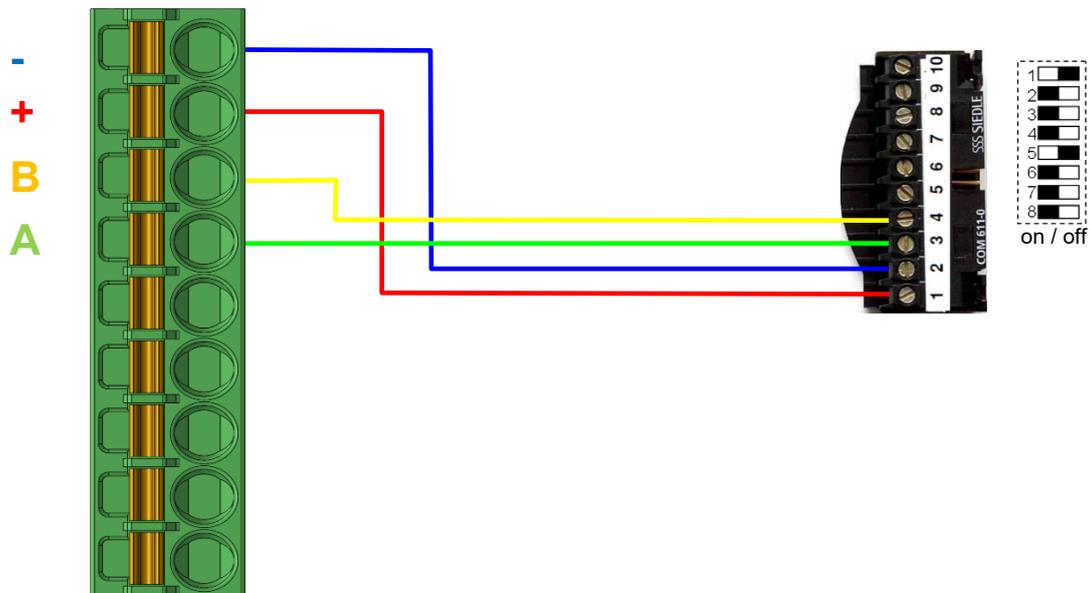


### Verdrahtungsplan für einen PHG-Leser

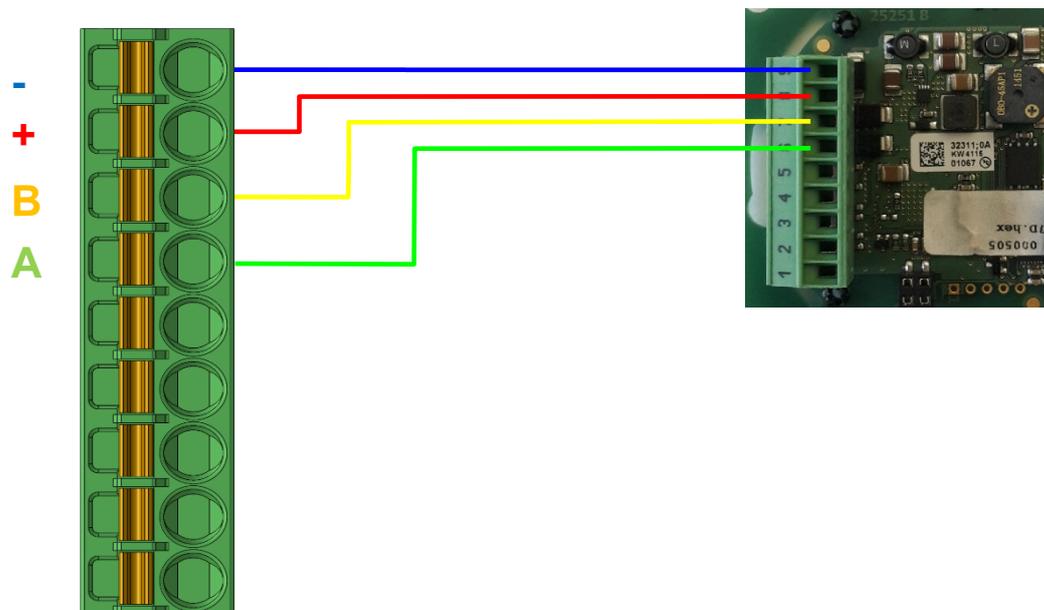
(hierbei gilt der gleiche Aufbau pro ZK-Strang bzw. ZM / Bus-ID)



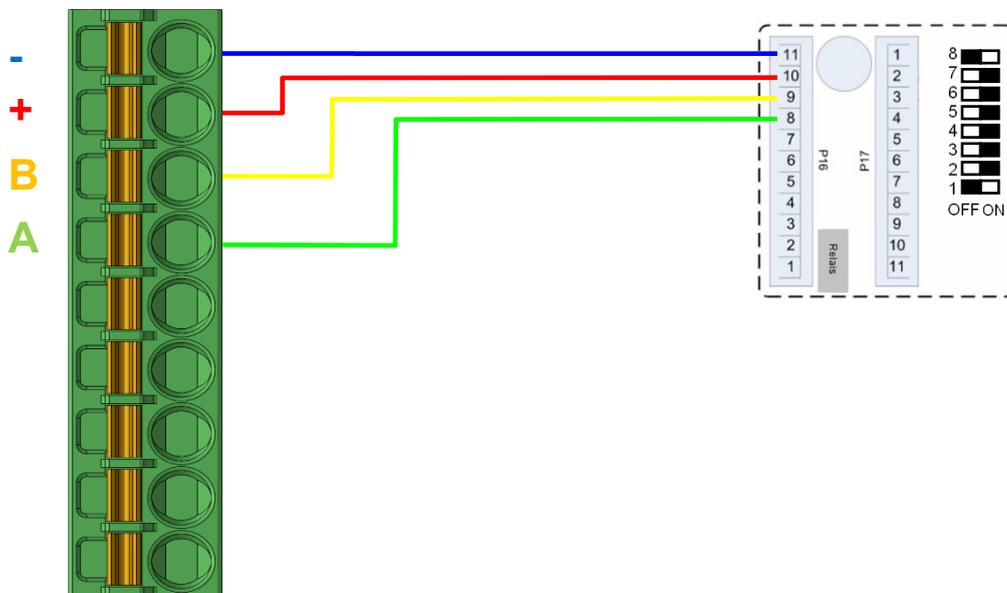
Verdrahtungsplan für einen Siedle-Leser  
(hierbei gilt der gleiche Aufbau pro ZK-Strang bzw. ZM / Bus-ID)



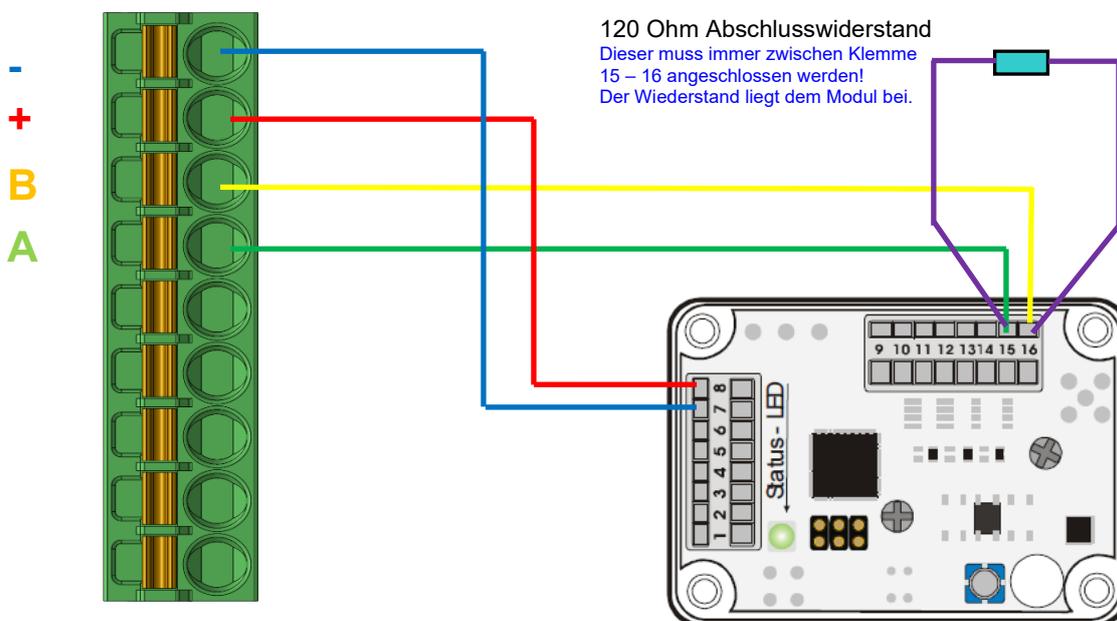
Verdrahtungsplan für einen Relino-B-ZK-Leser  
(hierbei gilt der gleiche Aufbau pro ZK-Strang bzw. ZM / Bus-ID)



## Verdrahtungsplan mit einem TS-Leser (hierbei gilt der gleiche Aufbau pro ZK-Strang bzw. ZM / Bus-ID)



## Anschluss eines U&Z Funkmoduls



### Hinweise bei der Verwendung von U&Z Funkmodulen:

Der Anschluss eines Funkmodules belegt beim Cenloc 4 Buss-Stränge.

#### Beispiel 1:

Wird an Busstrang 1 ein U&Z Funkmodul angeschlossen, so können am Bus 5, 9 und 13 kein Intera mehr genutzt werden.

Wird an Busstrang 3 ein U&Z Funkmodul angeschlossen, so können am Bus 7, 11 und 15 kein Intera mehr genutzt werden.

Gleiches gilt für Busstrang 3 und 4.

Beispiel Übersicht der RS485 Busstränge im Cenloc:

Bus NR 16	Bus NR 12 <b>ZK-Leser</b>	Bus NR 8 <b>ZK-Leser</b>	Bus NR 4 <b>ZK-Leser</b>
Bus NR 15 <b>ZK-Leser</b>	Bus NR 11 <b>ZK-Leser</b>	Bus NR 7 <b>ZK-Leser</b>	Bus NR 3 <b>U&amp;Z</b>
Bus NR 14 <b>ZK-Leser</b>	Bus NR 10	Bus NR 6	Bus NR 2 <b>ZK-Leser</b>
Bus NR 13 <b>ZK-Leser</b>	Bus NR 9 <b>ZK-Leser</b>	Bus NR 5 <b>ZK-Leser</b>	Bus NR 1 <b>U&amp;Z</b>

### Funkmodule= U&Z

Intera/PHG = **ZK-Leser** = OK

Intera/PHG = ~~ZK-Leser~~ = nicht möglich

**Beispiel 2:**

Wird an Busstrang 1 ein U&Z Funkmodul angeschlossen, so können am Bus 5, 9 und 13 kein Intera mehr genutzt werden.

Ein weiteres Funkmodul am Bus 5 ist möglich.

Beispiel Übersicht der RS485 Busstränge im Cenloc:

Bus NR 16	Bus NR 12 <b>ZK-Leser</b>	Bus NR 8 <b>ZK-Leser</b>	Bus NR 4 <b>ZK-Leser</b>
Bus NR 15 <b>ZK-Leser</b>	Bus NR 11	Bus NR 7 <b>ZK-Leser</b>	Bus NR 3 <b>ZK-Leser</b>
Bus NR 14 <b>ZK-Leser</b>	Bus NR 10	Bus NR 6	Bus NR 2 <b>ZK-Leser</b>
Bus NR 13 <b>ZK-Leser</b>	Bus NR 9 <b>ZK-Leser</b>	Bus NR 5 <b>U&amp;Z</b>	Bus NR 1 <b>U&amp;Z</b>

**Funkmodule= U&Z**

Intera/PHG = **ZK-Leser = OK**

Intera/PHG = **ZK-Leser = nicht möglich**

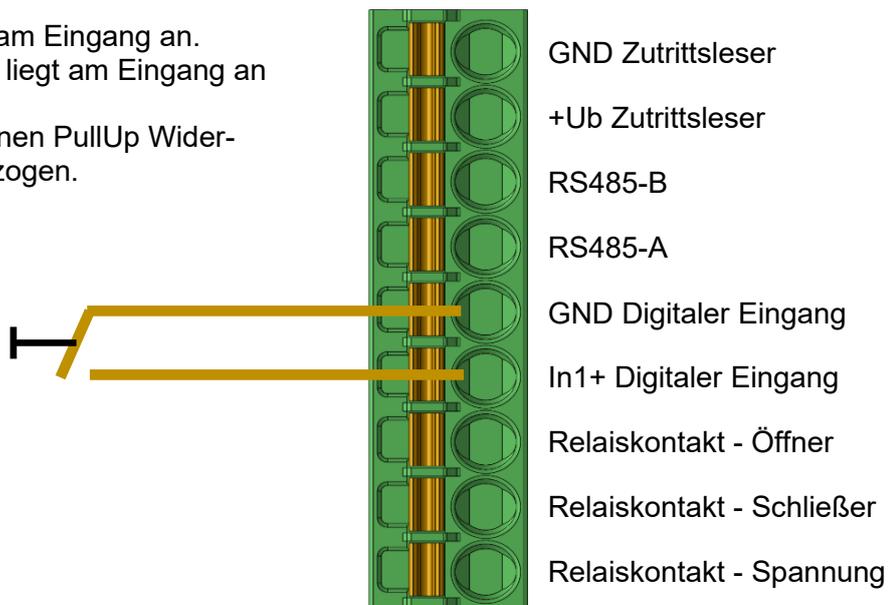
### 3.4.4. Digitaler Eingang am Steck-Modul

Taster (Bsp.)

Offen = „Hi“ liegt am Eingang an.

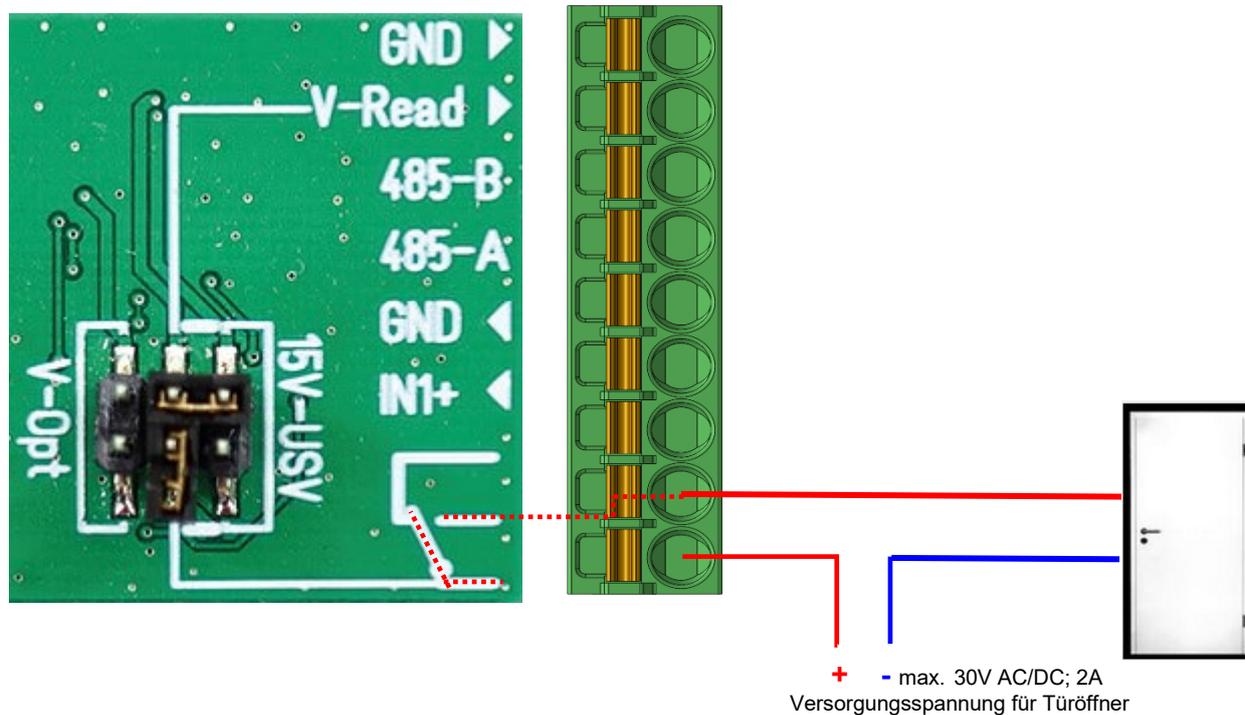
Gedrückt = „Low“ liegt am Eingang an

Der 1+ ist über einen PullUp Widerstand auf „Hi“ gezogen.

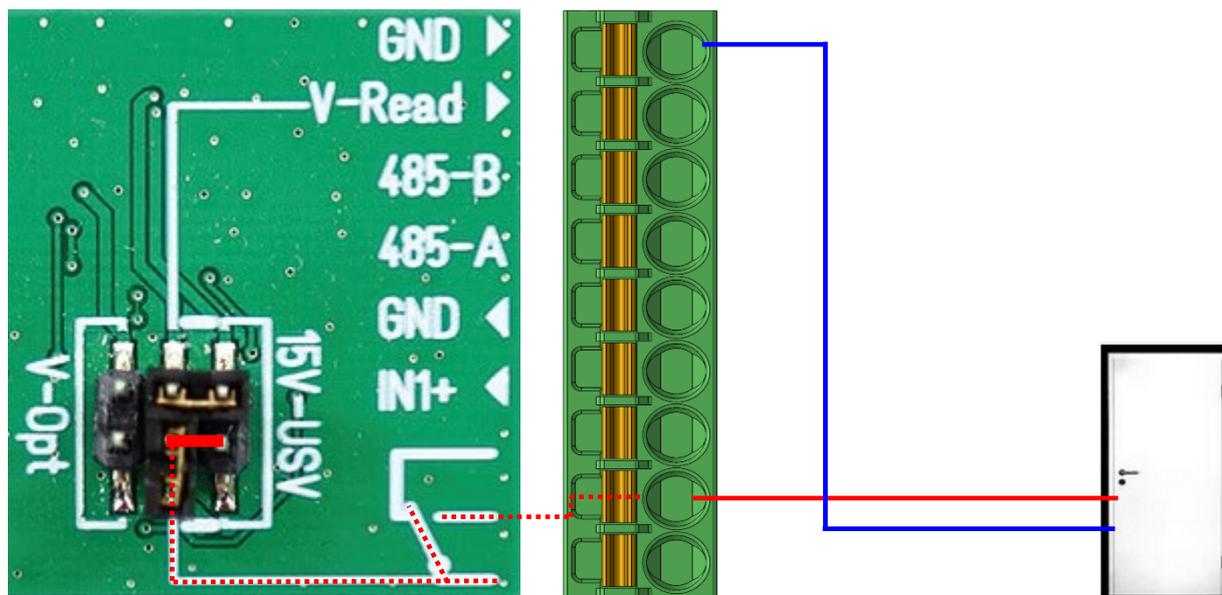


### 3.4.4.1. Anschluss eines Türöffners

#### Verdrahtung mit externer Spannungsversorgung – potentialfreier Anschluss



#### Verdrahtung für Versorgung des Türöffners über internes Hutschienennetzteil der CENLOC

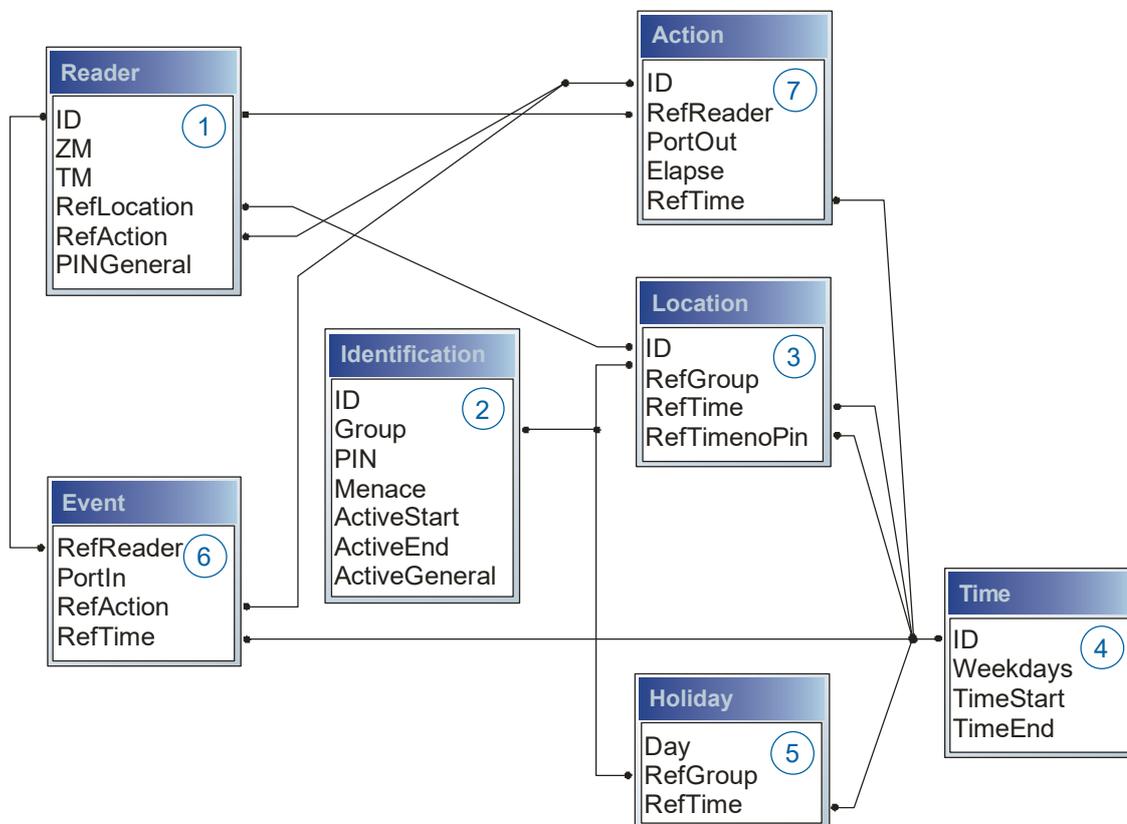




### 3.5. Anschluss der Zutrittskontrolle

#### 3.5.1. Konfiguration der ZK / Übersicht

**Grundlage** der Zutrittskontrolle II sind Tabellen. In ihnen werden alle Informationen über die Hardwarekonfiguration des Zutrittskontrollsystems, Zutrittsberechtigung des Personals, Zeiträume (Aktivierung, Sperrzeiten, Feiertage, ...) hinterlegt. Dabei besteht folgender Zusammenhang zwischen den einzelnen Tabellen:



Die Tabellen werden in Form von Text-Dateien erstellt. Innerhalb der Dateien können Sie zur leichteren Administration Kommentare einfügen.

Beim Einsatz von Kommentaren ist zu beachten, dass innerhalb einer Kommentarzeile keine Feldwerte angegeben werden können und die Kommentarzeile mit einem Semikolon beginnen muss.

Eine Reader.txt (Reader Tabelle) könnte wie folgt aussehen:

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

## Feiertagssteuerung

Es ist jetzt in der ZK-II möglich, Feiertage beim Schalten der Relais zu berücksichtigen. Um Kompatibilität mit den älteren Versionen zu erreichen, muss auf der Setupseite Zutrittskontrolle 2 die Funktion, „Feiertage bei der Zeitsteuerung der Relais“ berücksichtigen, aktiviert werden. Um den Tabellenaufbau der Holiday-Liste nicht ändern zu müssen, werden nun in der Spalte Group statt einer Gruppen-ID die Action-ID des geschalteten Relais-Ausgangs angegeben. In die Spalte RefTime ist das für diesen Tag geltende Zeitmodell hinterlegt. Damit das MasterIV-Terminal die Action-ID von der Gruppen-ID unterscheiden kann, muss ein Minuszeichen (-) vor die „Action-ID“ eingefügt werden, was zur Folge hat, dass diese Action-IDs nur noch 3-stellig sein dürfen.

### Beispiel:

#### Action

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

#### Holiday

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

In der o.g. Action-Liste ist dem Türmodul mit der ID 12 das Zeitmodell 2 zugeordnet, welches den Port 1 des Moduls schaltet. Ist die separate Feiertagssteuerung im Setup aktiviert worden, wird nun in diesem Beispiel am 1. Mai 2012 nicht das Zeitmodell 2 auf den Relais-Ausgang angewendet, sondern das Zeitmodell 5.

## Erweiterte Parametrierung ZK-II

Der Wertebereich des Parameters ‚ActiveGeneral‘ wurde um den Wert 8 erweitert. Zusätzlich zur Generalberechtigung (Wert 9) wird, falls beim Benutzer hinterlegt und beim Leser aktiviert, eine PIN-Abfrage durchgeführt. Weiterhin wird bei beiden Konfigurationen der Ausweise mit dem ActiveGeneral-Werten 8 und 9 der Gültigkeitszeitraum des Ausweises geprüft.

Für die ZK-II stehen die Betriebsarten online, offline oder online/offline nach Timeout zur Verfügung. Beim Onlinebetrieb werden, im Gerät hinterlegte Konfigurationslisten nicht berücksichtigt. Ein Datensatz wird vom Server gelesen, ausgewertet und eine Aktion ausgelöst. Beim Offlinebetrieb werden die Konfigurationslisten des Terminals verwendet, um einer Person Zutritt zu gewähren oder zu verweigern. Online/Offline nach Timeout ist eine Kombination. Ist der Server nicht erreichbar, kann das Terminal über seine Listen entscheiden, ob eine Person Zutritt erhält oder nicht.

## Zeitsteuerung der digitalen Ausgänge für die MasterIV-Geräteserie

Es ist möglich die digitalen Ausgänge der MasterIV-Geräteserie zeitlich über Tabellen zu steuern. So kann beispielsweise eine Nachtabsenkung der Heizanlage, eine Hupensteuerung und vieles mehr realisiert werden.

Folgende Tabellen müssen dazu konfiguriert werden:

- ▶ Action
- ▶ Reader
- ▶ Time



### Achtung:

In der Tabelle „Time“ empfehlen wir max. 64 Einträge für eine Zeitsteuerung zu verwenden.

### Beschreibung:

Jede auszulösende Aktion muss in der Tabelle „Action“ eingetragen werden. Die Tabelle „Action“ referenziert auf die Tabellen „Reader“ und „Time“. In der Tabelle „Reader“ wird das Modul hinterlegt, auf dem das Relais oder der Open Collector geschaltet werden soll.

Die Referenz auf die Tabelle „Time“ gibt an, wann geschaltet werden soll. Werden Start und Stoppzeitpunkt eingetragen, wird das Relais beim Überschreiten der Startzeit **ein-** und bei Überschreiten der Stoppzeit **ausgeschaltet**. Der Eintrag der Dauer **Elapse** in der Tabelle Action wird hierbei ignoriert.

Soll das Relais nur ein paar Sekunden auslösen, zum Beispiel für eine Hupensteuerung, muss die Stoppzeit auf „00:00“ gestellt werden. Wird nun die Startzeit überschritten, wird der entsprechende Ausgang für x Sekunden (RefTime in Action-Tabelle) geschaltet. Der Eintrag **Elapse** in der Tabelle „Action“ gibt jetzt die Einschaltdauer an.

### Beispiel:

Eine Hupe soll Montag bis Freitag morgens um **10.00** Uhr und nachmittags um **16.00** Uhr für **3** Sekunden auslösen. Die Hupe wird über das interne Relais des KYO Cenloc angesteuert.

Eine Heizungssteuerung soll an allen Wochentagen morgens um **07.00** Uhr in den „Tagbetrieb“ und abends um **19.00** Uhr in den „Nachtbetrieb“ geschaltet werden. Das entsprechende Relais befindet sich am Türmodul mit der Busnummer **2**.

### Reader.txt

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

### Time.txt

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

### Action.txt

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

### 3.5.2. Beschreibung der Tabellen für die Zutrittskontrolle 2

Tabelle **Reader** (Liste aller im System installierten Geräte)

Bezeichner	Datentyp	Länge	Beschreibung
ID	Nummer (int)	4	Eindeutiger Schlüssel (Wert>0) der Reader Tabelle.
ZM (Zutrittsmaster) bzw. BusNr. ID	Nummer (int)	4	Die Zutrittsmaster ID ist in unseren Beispielen immer 1. Existieren in einem Zutrittssystem z.B. mehrere MasterIV, können diese in einem Tabellenzusammenhang abgebildet werden und es ist nicht nötig für jeden MasterIV eine separate Liste zu pflegen. Kommen an einem Gerät mehrere Bus-Stränge RS485 zu Verwendung, muss jeder weitere Strang mit Master ID + 1 eingetragen werden.
TM	Nummer (int)	3	Die beiden linken Ziffern (010) geben die Busnummer des Türmoduls an, die rechte Ziffer (010) enthält die Information über die Anschlussart. Eine 0 an dieser Position bedeutet, Anschluss über RS485, eine 1 heißt Anschluss über RS232 oder RS485 als Stich (abgesetzter Leser).
RefLocation	Nummer (int)	4	Gibt an, welchen Raum der Leser überwacht.
RefAction	Nummer (int)	4	Gibt an welche Aktion nach erfolgreicher Prüfung abgearbeitet wird.
PinGeneral	Nummer (int)	8	Kann eine Zahlenreihe enthalten mit der eine Person ohne Ausweis Zutritt erhält.

Tabelle **Identification** (Liste aller bekannten Ausweise)

Bezeichner	Datentyp	Länge	Beschreibung
ID	Text (ASCII)	20	Enthält die Ausweis-Nr., welche am TMR33-Gerät oder Terminal gelesen wird. Ausweis kann mehrfach vorkommen (ist mehreren Berechtigungsgruppen zugeordnet).
Group	Nummer (int)	4	Ordnet den Ausweis einer Berechtigungsgruppe zu.
Pin	Nummer (int)	8	Aktiviert, wenn ungleich 0, eine Pin-Abfrage nach dem der RFID Ausweis gelesen wurde. Chip und PIN Kombination. 0=deaktiviert.
Duress/ Bedrohungscode	Nummer (int)	4	Aktiviert, wenn ungleich 0, eine an die Pin anfügbare „Bedrohungs-Pin“, Das System setzt im eingegebenen Falle einen Datensatz ab, der von einer entsprechend entwickelten Software ausgewertet werden kann und Polizeiruf oder Pfortneralarm auslöst.
ActiveStart	Text (Date)	10	Der hier eingetragene Tag gibt den Beginn der Gültigkeit für diesen Ausweis an. (z. B. 2018-07-12 = yyyy-mm-dd)
ActiveEnd	Text (Date)	10	Der hier eingetragene Tag gibt das Ende der Gültigkeit für diesen Ausweis an. (z. B. 2007-07-12 = yyyy-mm-dd)
ActiveGeneral	Nummer (int)	1	Aktiviert oder deaktiviert diesen Ausweiseintrag. 0 = Ausweis gesperrt 1 = Ausweis aktiv 2 = Virtueller Ausweis (Verwendung nur über DLL oder http response) 3 = Zutritt nur über PIN Eingabe; Feld ID wird zu Pin, Feld Pin = 0 4= Pin = Bedrohungscode d.h. der Bedrohungscode wird anstelle der Pin eingegeben. 5= Der Wert bei Duress/Bedrohungscode wird ohne Übertrag auf die PIN aufaddiert und bildet so den Bedrohungscode (bsp: Pin=1234, Duress=1 -> Bedrohungscode=1235; Pin=1234, Duress=6 -> Bedrohungscode=1230) 6= Daueröffnung bei U&Z-Zylindern 7 = EMA Schaltberechtigung 8 = Generelle Berechtigung (mit PIN-Abfrage) 9 = Generelle Berechtigung (keine PIN-Abfrage)

**Tabelle Location** (legt fest, welche Ausweisgruppe zu welcher Zeit in welchen Raum Zutritt erhält)

Bezeichner	Datentyp	Länge	Beschreibung
ID	Nummer (int)	4	ID des Raumes. Über diese Nummer nehmen alle anderen Tabellen bei Bedarf auf diese Datenzeile Bezug.
RefGroup	Nummer (int)	4	Verweis auf die Tabelle Identification. Kennzeichnet die zutrittsberechtigten Gruppe. Alle Ausweise dieser Gruppe haben zu diesem Raum Zutritt.
RefTime	Nummer (int)	4	Das Zeitmodell, in welchem berechnete Personen Zutritt erhalten. (0 = darf nicht verwendet werden)
RefTimeNoPin	Nummer (int)	4	Das Zeitmodell, zu dem eine zusätzliche PIN nicht eingegeben werden muss (in Stoßzeiten, etc.).

**Tabelle Time** (legt Zeitmodelle unter einer Nummer fest mit Wochentag und Gültigkeit von - bis)

Bezeichner	Datentyp	Länge	Beschreibung
ID	Nummer (int)	4	ID des Zeitmodells. Über diese Nummer nehmen alle anderen Tabellen, bei Bedarf, auf diese Datenzeile Bezug. ! Bei automatischer Zeitsteuerung werden nur die ersten 32 Einträge genutzt.
Weekdays	Nummer (int)	7	Gibt die Wochentage an, in welchen der nachfolgende Zeitraum gelten soll. Format: Max. 7 Stellen 1-7 z.B. 134567 = Montag, Mittwoch bis Sonntag)
TimeStart	Text (Time)	5	Der Startzeitpunkt für den Zeitraum. (Format 24h HH:MM)
TimeEnd	Text (Time)	5	Der Endzeitpunkt für den Zeitraum.

**Tabelle Holiday** (Festlegung von Sperrtagen, Feiertage und Betriebsurlaub)

Bezeichner	Datentyp	Länge	Beschreibung
Day	Text (Date)	10	Datum des Sperrtages. (Format: YYYY-MM-DD) Ist ein Sperrtag hinterlegt, gilt dieser erstmal immer für alle Gruppen.
RefGroup	Nummer (int)	4	Soll eine Gruppe an einem Sperrtag Zutritt erhalten, kann das hier definiert werden. Nur im Zusammenhang mit einem Zeitmodell.
RefTime	Text (Time)	4	Gibt das zugeordnete Zeitmodell an (0 = wird nicht verwendet). Während dieser Zeit wird der Zutritt gewährt. Hierdurch können auch „halbe Feiertage“, wie Silvester realisiert werden.

**Tabelle Event** (Zuordnung einer Action zu einem Signal an einem digitalen Eingang)

Bezeichner	Datentyp	Länge	Beschreibung
RefReader	Nummer (int)	4	Modul (Türmodul oder Master) auf dem sich der digitale Eingang befindet.
PortIn	Nummer (char)	1	Nummer des digitalen Eingangs auf dem Modul. Schaltet der digitale Eingang von Low auf Hi wird das Event ausgeführt.
RefAction	Nummer (int)	4	Referenz auf die Action, die ausgeführt werden soll (z. B. ein Relais schalten).
RefTime	Nummer (int)	4	Das Zeitmodell, welches angibt, wann der digitale Eingang geprüft wird. (0 = darf nicht verwendet werden, der Eintrag ist sonst ungültig)

**Tabelle Action** (Liste aller ausführbaren Aktionen im Zutrittskontrollsystem. Eine Aktionsgruppe, alle Aktionen mit gleicher Aktionsnummer, kann mehrere Relais schalten.)

Bezeichner	Datentyp	Länge	Beschreibung
ID	Nummer (int)	4	Aktionsnummer, sie kann aufgrund mehrerer abzuarbeitender Aktionen mehrfach vorkommen.
RefReader	Nummer (int)	4	Modul (Türmodul oder Master) auf dem ein Ausgang (Relais) geschaltet wird.
PortOut	Nummer (char)	1	Gibt die Nummer des Ausgangs auf dem Modul an. Mögliche Angaben: 1 ... 9 & A ... W entspricht Port 1-32 (digital out)
Elapse	Nummer (int)	3	Die Dauer, für die das Relais geschaltet wird (0 nicht verwendet). Einheit 200 ms
RefTime	Nummer (int)	4	Das Zeitmodell gibt an, wann der Ausgang dauerhaft geschaltet wird. (0 = wird nicht verwendet). Wird ein Zeitmodell angegeben, so wird diese Aktion zur angegebenen Zeit durchgeführt. (Automatische Zeitsteuerung) Bei einer Zeitangabe (1 1234567 00:00-23:59) ist der Ausgang 24h 7 Tage eingeschaltet. <b>! Aktionen die hier ausgeführt werden, dürfen nicht mit Zutrittsaktionen gemischt werden!</b>

### 3.5.3. Anschlussvarianten für den Datafox KYO Cenloc

Der KYO Cenloc kann optional mit bis zu 16 ZK-Busanschlüssen RS485 ausgestattet werden. Pro RS485-Bus können bis 16 Leser angeschlossen werden. Maximal dürfen 64 ZK-Leser an die Zentrale angeschlossen werden.

Dadurch entstehen vielfältige Anschlussvarianten für den Aufbau einer Zutrittskontrolle.

#### 3.5.3.1. Sternförmiger Aufbau der ZK für den Datafox KYO Cenloc

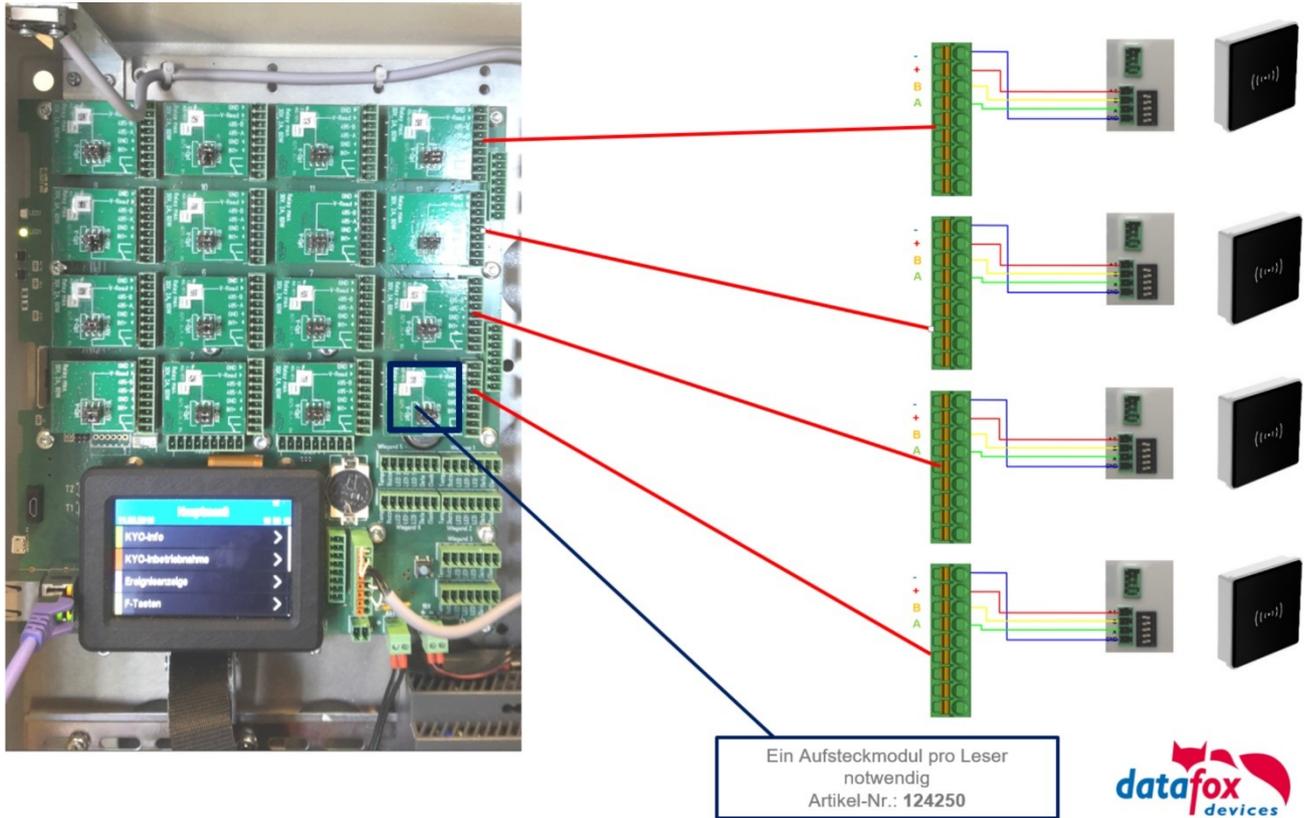
Empfohlen ist dabei dieser Aufbau:

max. 16 Leser, Sternförmig und pro Leser ein RS485 Aufsteckmodul.

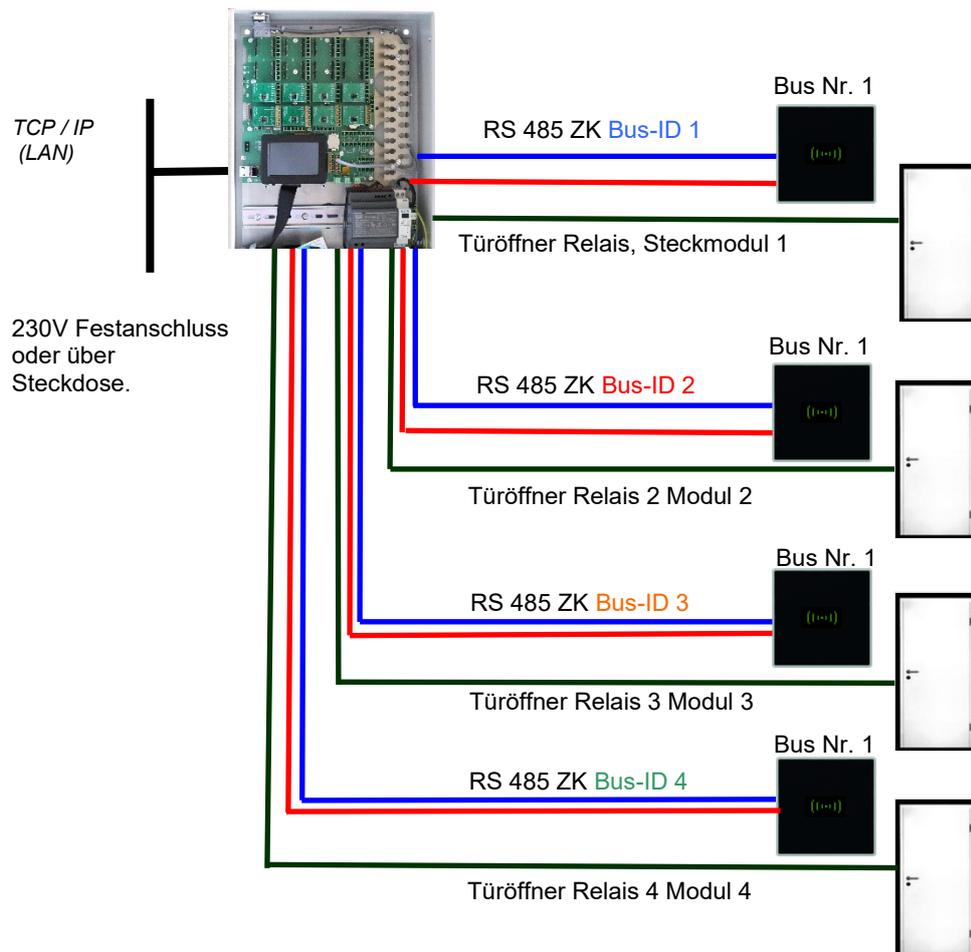


### 3.5.3.2. Sternförmiger Aufbau mit 4 Lesern

Anschluss Übersicht:



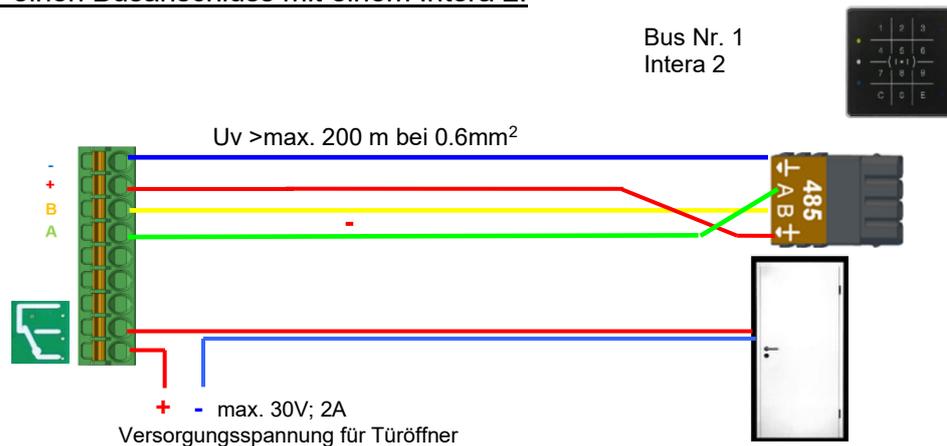
### Verkabelungsplan für 4 Türen, 4 Relais im KYO Cenloc:



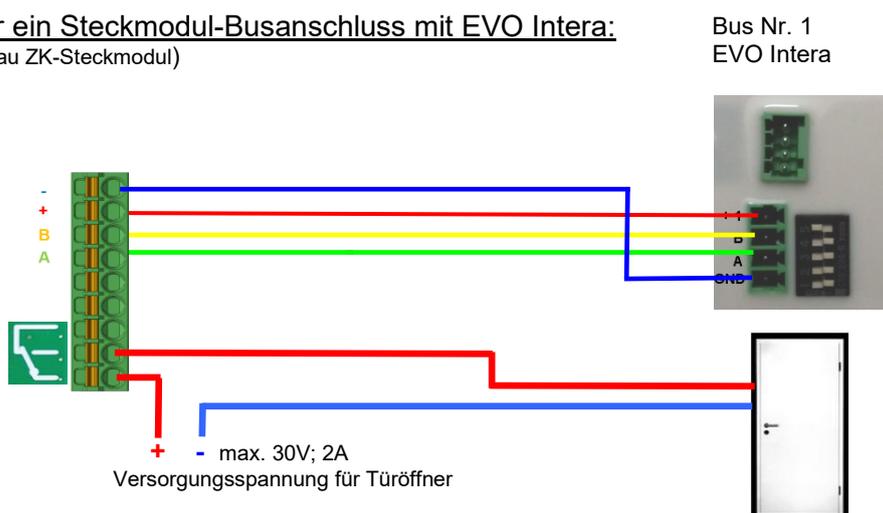
#### Entsprechende Reader Tabelle, Beispiel:

ID	ZM / Bus-ID	TM (Busadresse)	RefLocation	RefAction	PinGeneral	Beschreibungstext
1	1	010	1	1	0	Leser an RS485 Steckplatz 1 = Bus ID 1
2	2	010	2	2	0	Leser an RS485 Steckplatz 2 = Bus ID 2
3	3	010	3	3	0	Leser an RS485 Steckplatz 3 = Bus ID 3
4	4	010	4	4	0	Leser an RS485 Steckplatz 4 = Bus ID 4
Bis 16 Leser sind auf diese Weise anschließbar. Der Leser wird vom Cenloc mit Spannung versorgt!						
5	5	010	5	5	0	Leser an RS485 Steckplatz 5 = Bus ID 5
--						
16	16	010	16	16	0	Leser an RS485 Steckplatz 16 = Bus ID 16
99	1	320	0	1	0	KYO Cenloc V4 (Mastergerät=Cenloc selbst)

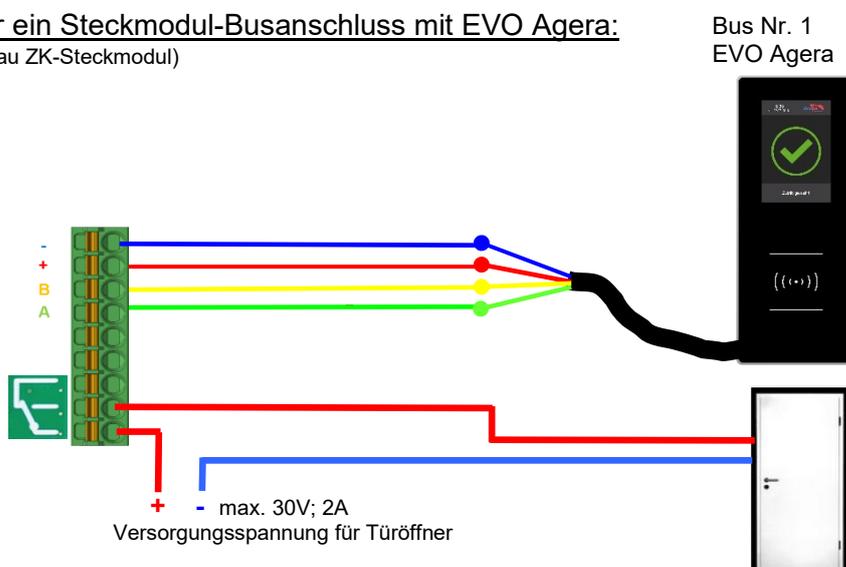
Verdrahtungsplan für einen Busanschluss mit einem Intera 2:



Verdrahtungsplan für ein Steckmodul-Busanschluss mit EVO Intera:  
(hierbei gilt der gleiche Aufbau ZK-Steckmodul)

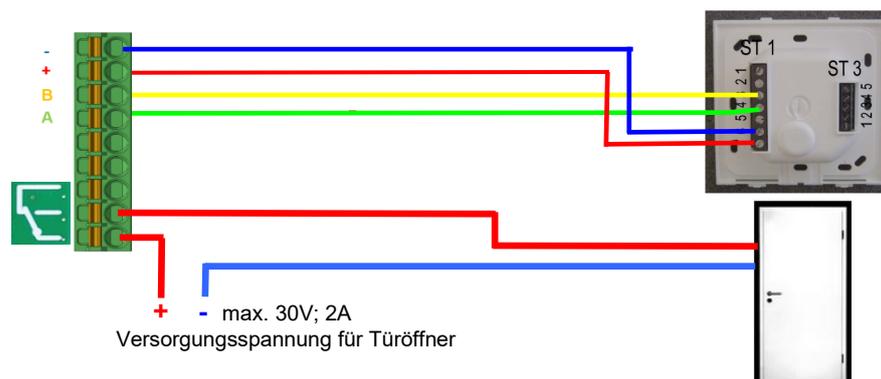


Verdrahtungsplan für ein Steckmodul-Busanschluss mit EVO Agera:  
(hierbei gilt der gleiche Aufbau ZK-Steckmodul)



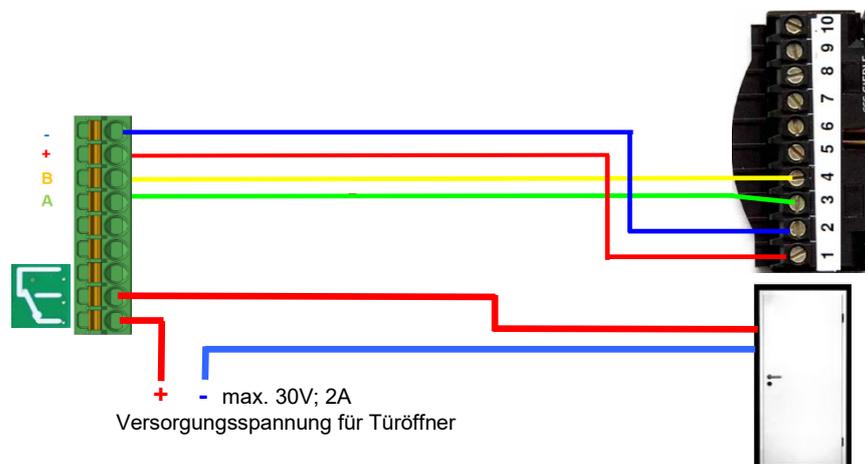
Verdrahtungsplan für ein Steckmodul-Busanschluss mit EVO Intera:  
(hierbei gilt der gleiche Aufbau ZK-Steckmodul)

Bus Nr. 1  
EVO Intera



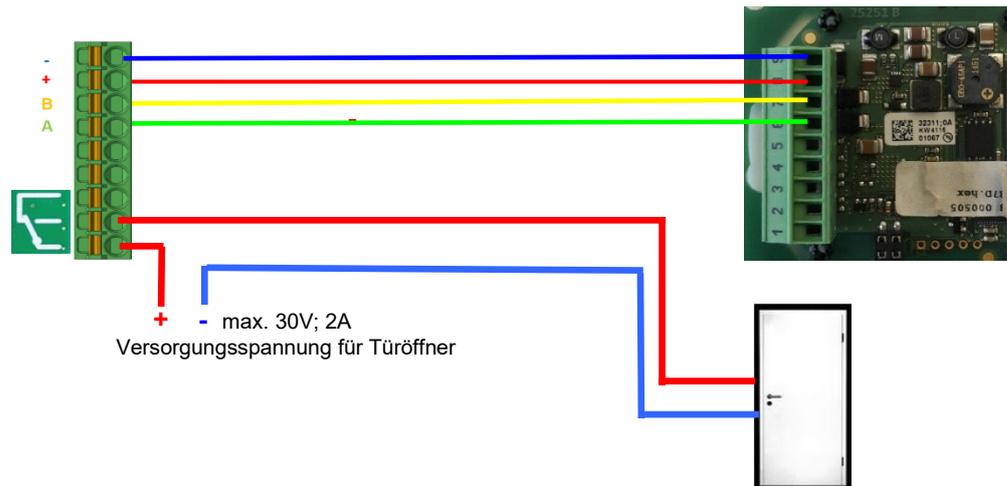
Verdrahtungsplan für ein Steckmodul-Busanschluss mit PHG-Siedle:  
(hierbei gilt der gleiche Aufbau ZK-Steckmodul)

Bus Nr. 1  
Siedle-Leser



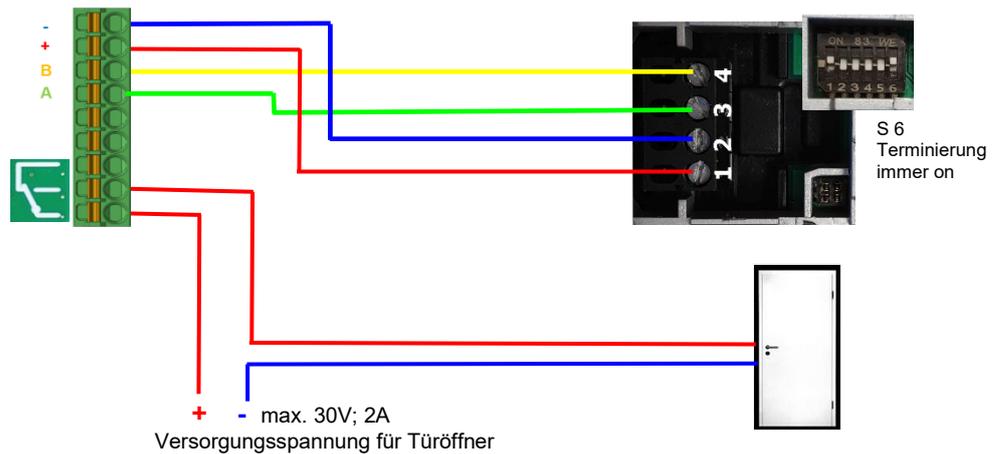
Verdrahtungsplan für ein Steckmodul-Busanschluss mit Relino-B:  
(hierbei gilt der gleiche Aufbau ZK-Steckmodul)

Bus Nr. 1  
Relino-B



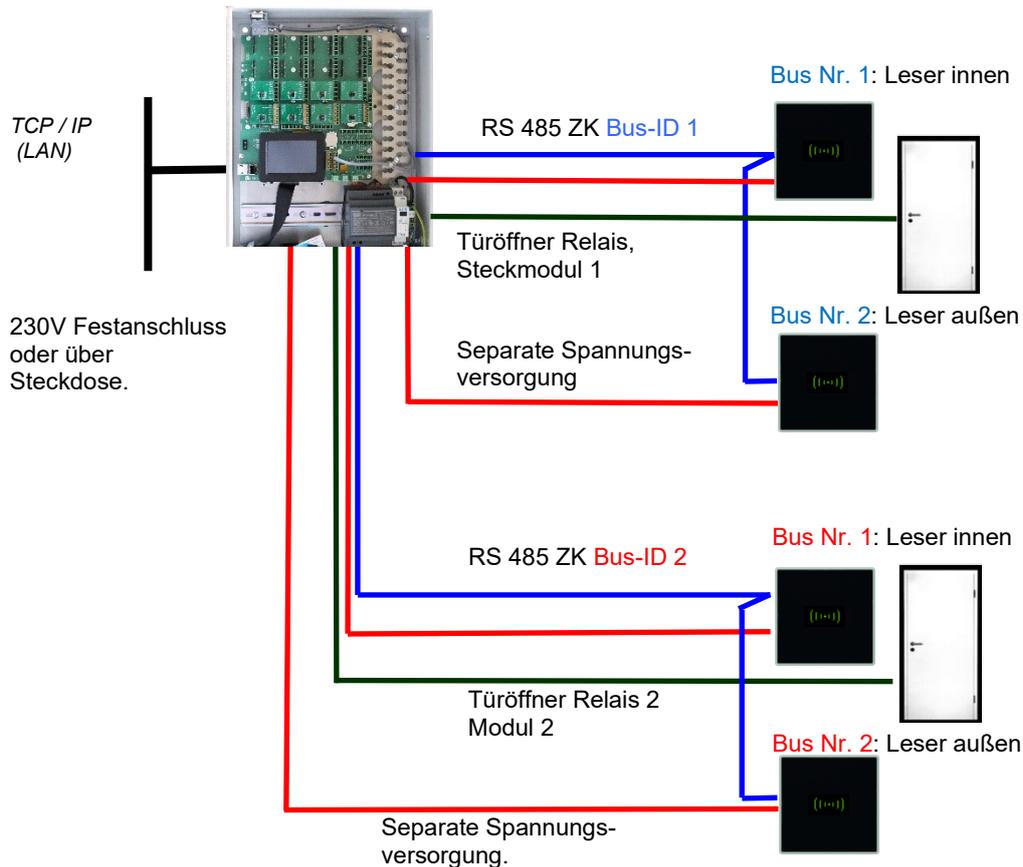
Verdrahtungsplan für ein Steckmodul-Busanschluss mit PHG VOXIO-T-Z-Leser:  
(hierbei gilt der gleiche Aufbau pro ZK-Strang bzw. ZM / Bus-ID)

Bus Nr. 1  
PHG-VOXIO-T-Z-Leser



### 3.5.3.3. 2 x RS485 Bus, 4 Leser an 2 Tür innen/außen

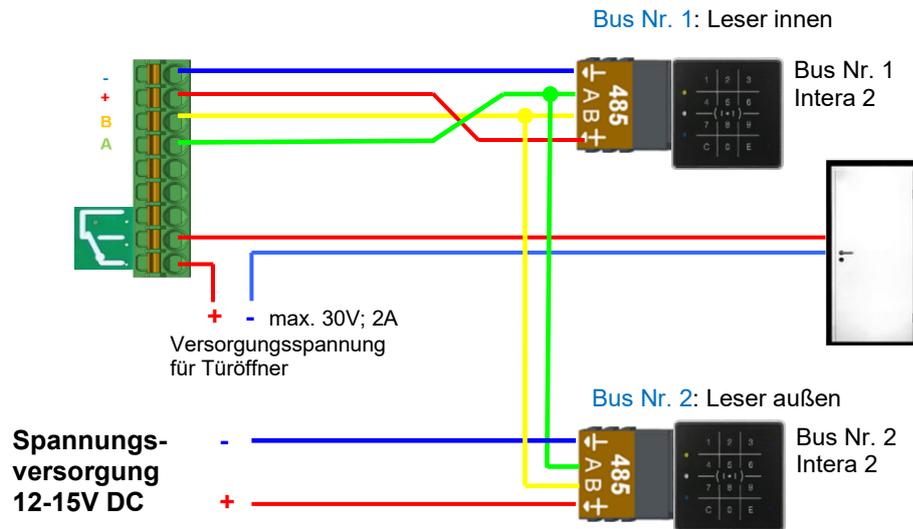
Verkabelungsplan für 2 Türen, 2-Leser an einem RS485 KYO Cenloc:



Entsprechende Reader Tabelle, Beispiel:

ID	ZM / Bus-ID	TM (Busadresse)	RefLocation	RefAction	PinGeneral	Beschreibungstext
1	1	010	1	1	0	Leser an RS485 Steckplatz 1 = Bus ID 1
2	1	020	2	1	0	Leser an RS485 Steckplatz 2 = Bus ID 2
3	2	010	3	3	0	Leser an RS485 Steckplatz 3 = Bus ID 3
4	2	020	4	3	0	Leser an RS485 Steckplatz 4 = Bus ID 4
Bis 32 Leser sind auf diese Weise anschließbar. Es wird nur je ein Leser vom Cenloc (Steckmodul) mit Spannung versorgt! Der zweite Leser muss an (direkt an 12V) eine Separate Spannungsversorgung angeschlossen werden.						
99	1	320	0	1	0	KYO Cenloc V4 (Mastergerät=Cenloc selbst)

Verdrahtungsplan für einen Busanschluss mit 2 Lesern (Intera 2):

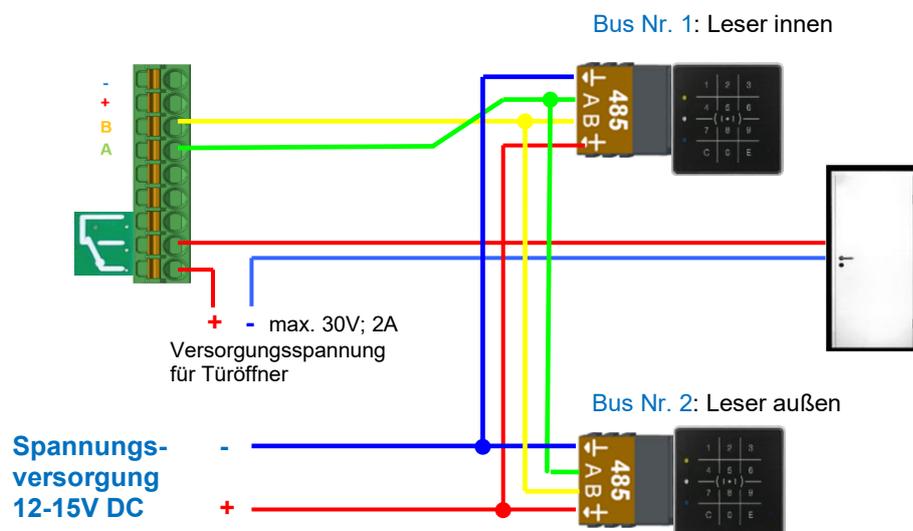


**Achtung:**

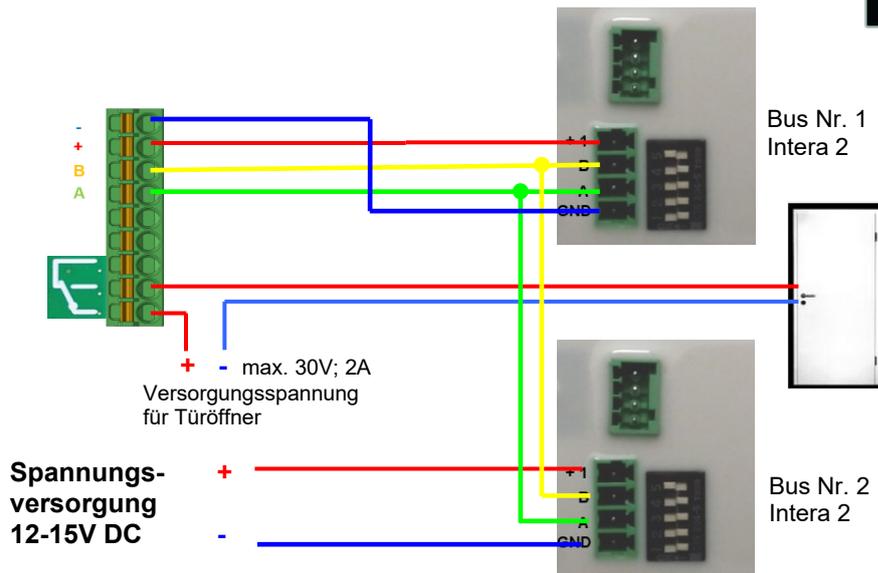


Die Spannungsversorgung des Steckmoduls  kann nur ein externes Gerät versorgen! Eine Versorgung von 2 Lesern oder Leser+Onloc ist nicht möglich.

Verdrahtungsplan für einen Busanschluss mit 2 Lesern (Intera 2)  
Mit separaten Spannungsversorgung für beide Leser:

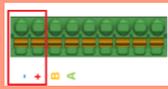


Verdrahtungsplan für einen Busanschluss mit 2 Lesern (Intera):

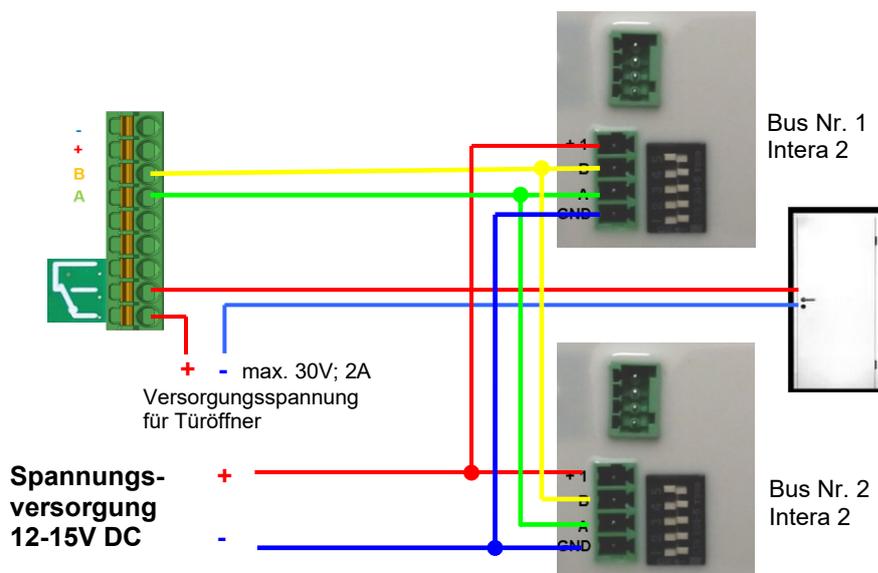


**Achtung:**



Die Spannungsversorgung des Steckmoduls  kann nur ein externes Gerät versorgen! Eine Versorgung von 2 Lesern oder Leser+Onloc ist nicht möglich.

Verdrahtungsplan für einen Busanschluss mit 2 Lesern (Intera):  
Mit separaten Spannungsversorgung für beide Leser:

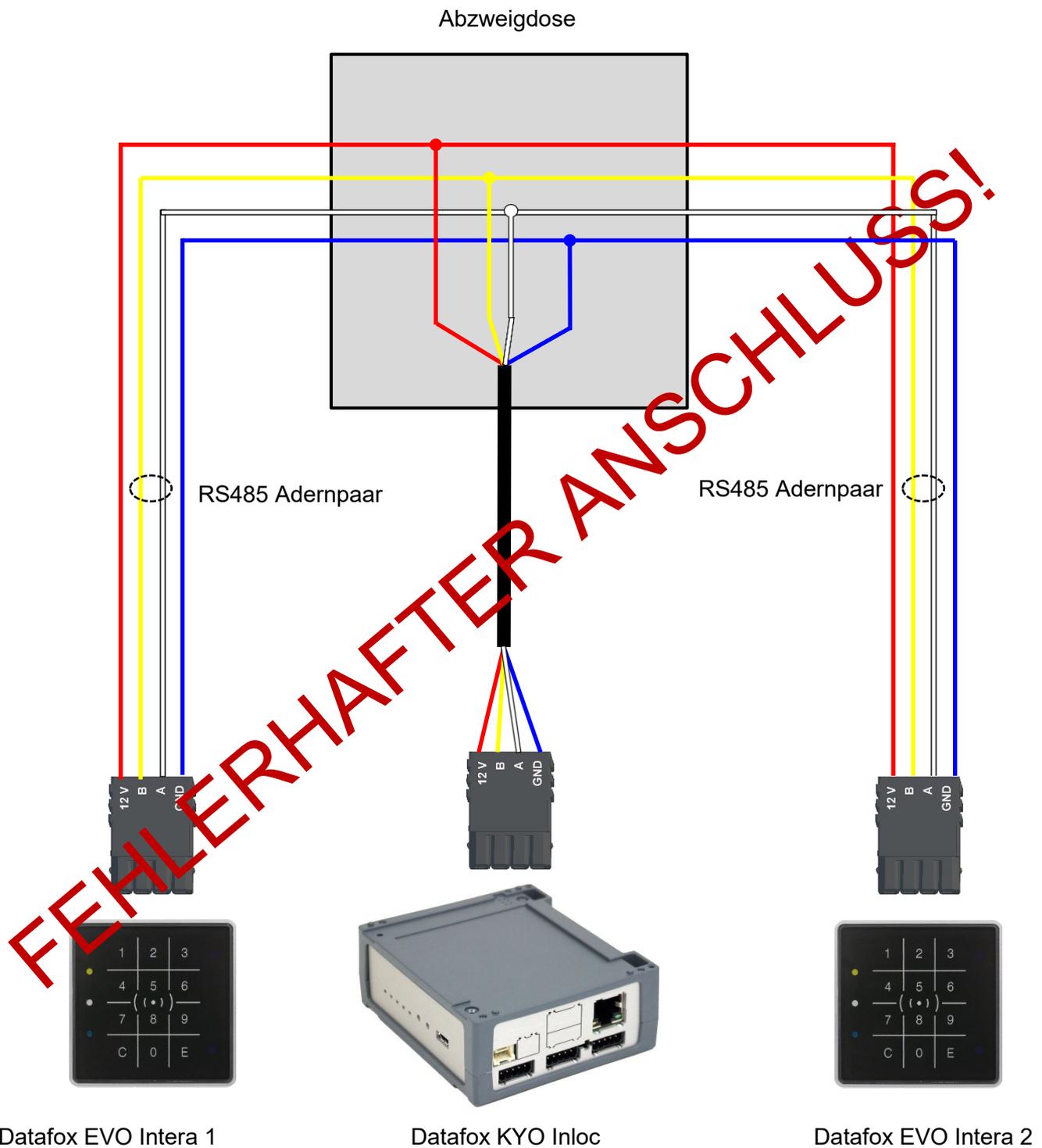




### 3.5.4. Hinweise für den Elektriker zur Installation der Zutrittskontrolle

#### 3.5.4.1. Busverkabelung Sternförmig

**! Falscher sternförmiger Anschluss des RS485-Busses.  
RS485 Adernpaare dürfen nicht parallel geschaltet werden.**



Datafox EVO Intera 1

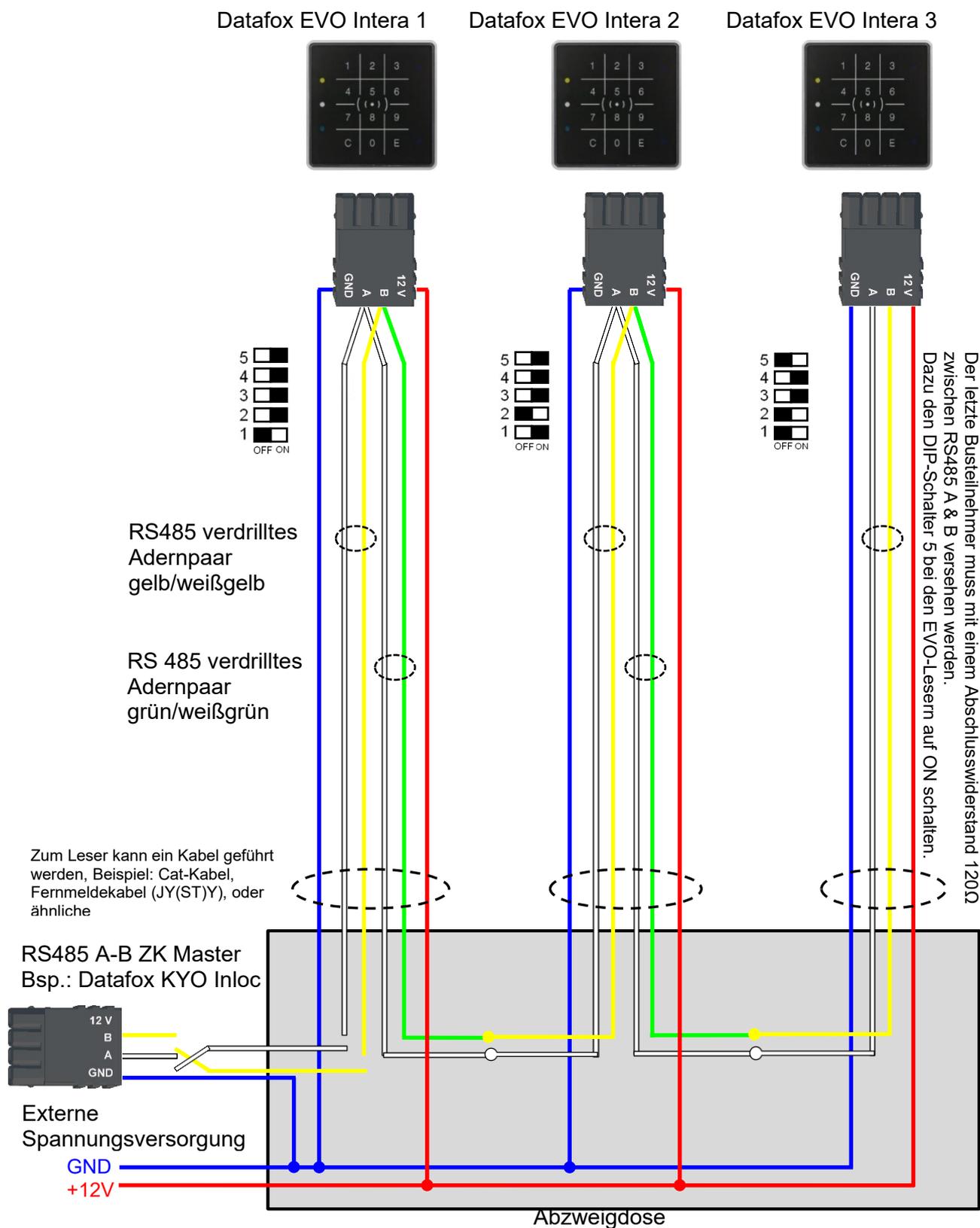
Datafox KYO Inloc

Datafox EVO Intera 2

## RICHTIG!

### Korrekte Busverdrahtung der Zutrittsleser bei sternförmiger Kabelverlegung.

Die Verdrahtung darf nicht parallel von einem Punkt aus geschehen. Die Adernpaare A und B müssen jeweils in Reihe direkt zur Anschlussklemme eines Lesers geführt und von dort weiter zum nächsten Busteilnehmer geschliffen werden, um ein reibungsloses Arbeiten des Busses gewährleisten zu können.



### 3.5.5. Zutrittskontrolle II mit EVO Intera II

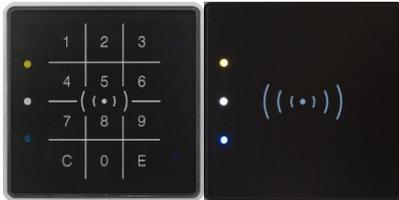
Folgende Hardware steht für den Aufbau einer Zutrittskontrolle mit EVO-Intera 2 zur Verfügung. Entsprechend der Hardwareanforderung der einzelnen Geräte können diese in verschiedenen Varianten miteinander kombiniert werden.

KYO Cenloc

Wird das MasterIV-Gerät für die Zutrittskontrolle, Tür- bzw. Fernüberwachung eingesetzt, können mit einem Gerät bis zu 8/16 Türen überwacht und gesteuert werden.

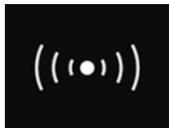
#### EVO Intera

##### Ohne und mit PIN



Unterputz: 81 x 81 x 19 mm (BxHxT)

Der Intera 2 Leser kann mit 125kHz, Legic bzw. Mifare eingesetzt werden. Er ist als Aufputzvariante erhältlich. Jeder Leser besitzt ein Leuchtfeld zur Visualisierung des Status und einen Buzzer zur akustischen Signalisierung.



Signalisierung der Hintergrundbeleuchtung:  
 Weiß leuchtend = Leser Betriebsbereit  
 Weiß blinkend = Leser nicht erkannt



Signalisierung der Hintergrundbeleuchtung:  
**grün** = Zutritt gestattet



Signalisierung der Hintergrundbeleuchtung:  
**rot** = Zutritt verweigert oder Leser wird gerade vom Master Konfiguriert. Oder Leser wurde erkannt aber nicht in der Reader eingetragen.



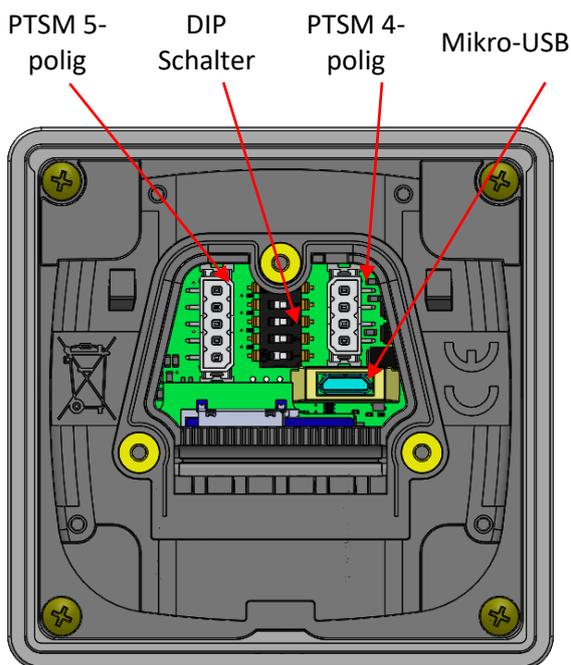
LED – **Gelb** Transponder im Feld

LED – **Weiß** = Leser im Schlafmodus (Abgeschaltet durch den Näherungssensor.)  
 LED – Aus Lesebereit und die Hintergrundbeleuchtung RFID-LED ist an.

LED – **Blau** (noch keine Funktion)

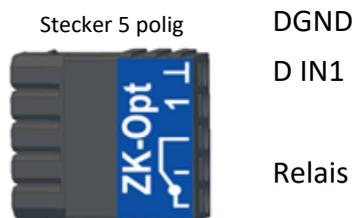
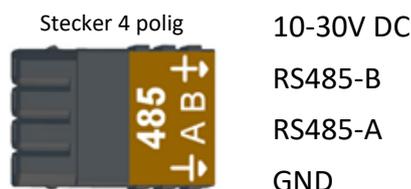
## Anschlussbelegung:

### Anschlussbelegung



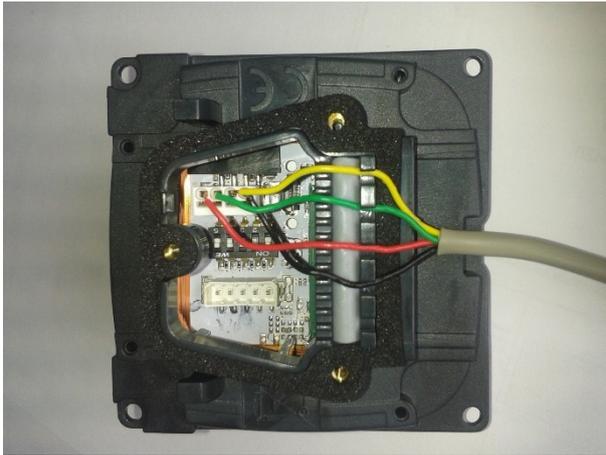
#### Anschluss an die PTSM Steckverbinder Connection to the PTSM connector

Im Lieferumfang des EVO Intera II sind der 4-polige bzw. 5-polige Gegenstecker zum Anschluss des Lesers enthalten. Diese sind verpolungssicher und werden von Datafox mit aufgedruckter Belegung ausgeliefert.



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 – Abschlusswiderstand 120R	Inaktiv	aktiv

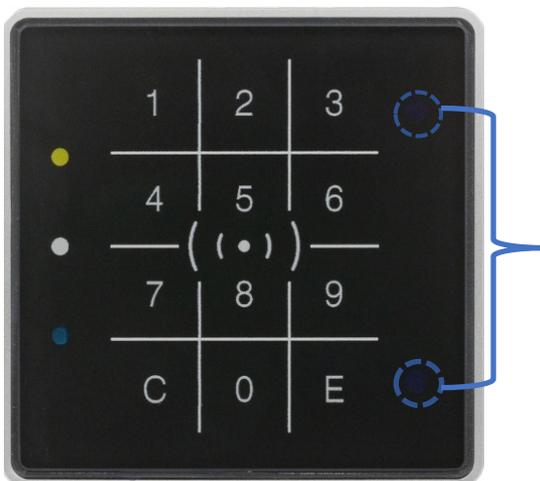
Beispiel	5-4-3-2-1
Adresse 2, mit Abschlusswiderstand	1-0-0-1-0
Adresse 3, ohne Abschlusswiderstand	0-0-0-1-1



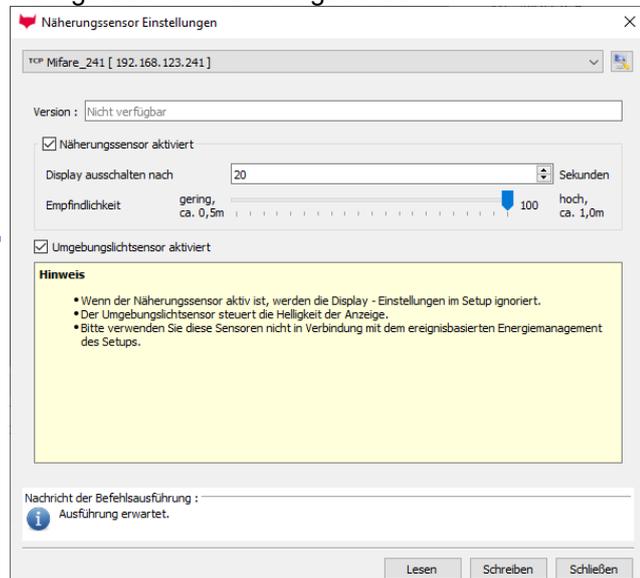
### Verdrahtung

Der EVO Intera II verfügt über einen integrierten Kabelkamm zur Aufnahme von Einzeladern bis  $d=1,5\text{mm}$  inkl. Einhängung zur Zugentlastung. Adern wie dargestellt verlegen.

### Einstellung des Näherungssensors:



Der Näherungssensor befindet sich am rechten Rand: Die Einstellung erfolgt über das DatafoxStudioIV unter Konfiguration -> Näherungssensor:



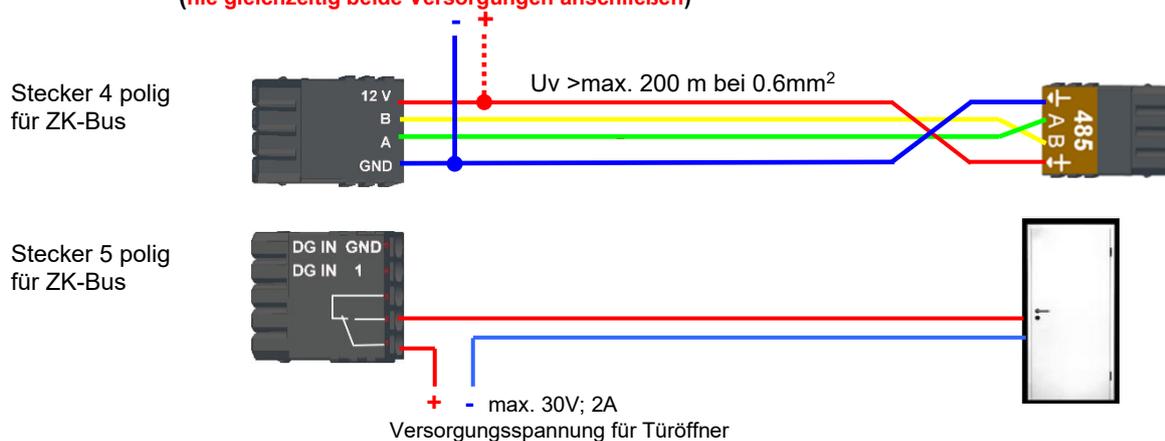
Entsprechende Reader Tabelle, Beispiel:

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)

### Verdrahtungsplan für einen Busanschluss mit einem Intera 2:

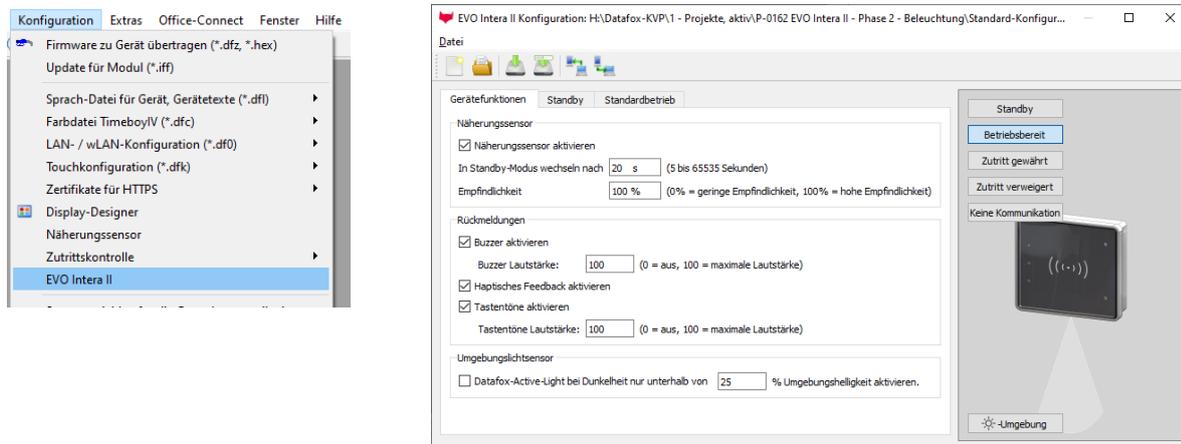
Optional: Spannungsversorgung über Netzteil 12 V DC. Immer notwendig, wenn mehr als ein Leser an einem RS485 Anschluss angeschlossen ist.  
**(nie gleichzeitig beide Versorgungen anschließen)**

Bus Nr. 1  
EVO Intera II Leser



### 3.5.5.1. EVO Intera II, Individuelle Einstellungen

Die Maske zum Einstellen der EVO Intera II Konfiguration ist im Datafox Studio über das Konfigurationsmenü zugänglich:



Die Maske erlaubt das Einstellen/Anpassen des Verhaltens des EVO Intera II. Diese Einstellungen sind in drei Bereiche unterteilt:

- Konfiguration der Geräte-Sensoren und -Aktoren (Reiter Gerätefunktionen)
- Konfiguration der Standby-Konfiguration (Unterkonfiguration des Näherungssensors)
- Konfiguration des Normalbetriebs (Reiter Standardbetrieb)

Zusätzlich wird – bezogen auf einen gewählten Betriebszustand – eine Vorschau der Leser-Signalisierung dargestellt.

#### Funktionsweise des EVO Intera II

Der EVO Intera II ist ein RFID-Leser für den Einsatz in der Zutrittskontrolle. Als solcher ist er auf den Betrieb an einem RS485-Bus ausgelegt und nutzt das phg\_crypt Kommunikationsprotokoll, das in weiten Teilen der Industrie als Defacto-Standard eingesetzt wird.

Der Leser unterscheidet sich hinsichtlich seiner Ausstattung von vielen Konkurrenzprodukten:

- Er kann indirekte Beleuchtung projizieren.
- Er verfügt über Sensorik zur Umgebungslicht- und Näherungserkennung.
- Er kann als Pin-Leser eingesetzt werden und dann zusätzlich zum akustischen Feedback auch haptisches Feedback erzeugen.

Ferner verfügt der EVO Intera II über drei programmierbare LEDs auf der linken Seite. Diesen LEDs können Funktionen zugeordnet werden, wie beispielsweise das Signalisieren eines Ausweises im Feld des RFID-Lesers oder einer Person in der Nähe. Es gibt auch weitere Funktionen wie dauerhaft an/aus oder vom Zutrittscontroller geschaltet.

Zur Einrichtung dieser Merkmale dient der in diesem Kapitel beschriebene Dialog des Datafox Studios. Die Übertragung der Konfiguration erfolgt über die USB-Schnittstelle des Lesers.

## Globale Funktionen

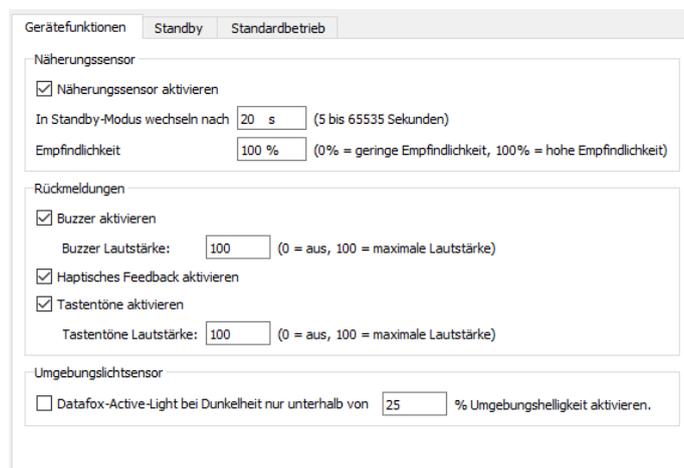


Die Maske bietet von links nach rechts Funktionen zum

- Erstellen einer neuen Standard-Konfiguration
- Einlesen einer Konfigurationsdatei
- Speichern der Konfigurationsdatei
- Speichern der Konfigurationsdatei unter einem neuen Namen
- Übertragen der Konfigurationsdatei auf einen EVO Intera II
- Lesen der Konfigurationsdatei aus einem EVO Intera II

Diese Aktionen sind ebenfalls für das Datei-Menü zugänglich.

## Einstellung der Gerätefunktionen



Der EVO Intera II verfügt über einen Näherungssensor – ist dieser aktiviert, so kann die Standby-Beleuchtung festgelegt werden. Der Standby-Modus wird aktiviert, wenn für einen einstellbaren Zeitraum (20 Sekunden im Standard) keine Person in der Nähe des Lesers erkannt wird.

Je nach baulicher Situation kann es erforderlich sein, den Näherungssensor in seiner Empfindlichkeit einzuschränken, etwa wenn er in schmalen Gängen eingesetzt wird und die gegenüberliegende Wand vermeintlich als Person in der Nähe erkannt wird.

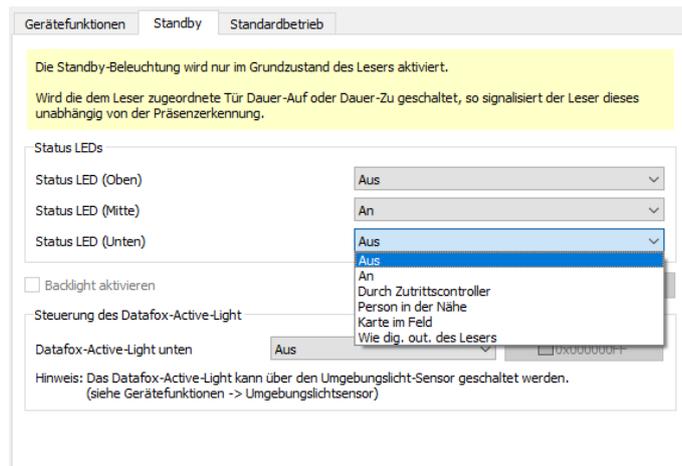
Als Rückmeldungen stehen neben dem

- Buzzer für Zutrittsereignisse noch
- Haptisches und Ton-Feedback bei PIN-Lesern bereit.

Für alle akustischen Rückmeldungen können Sie die maximale Lautstärke einstellen, so dass der Leser auch an ruhige Büro-Umgebungen angepasst werden kann.

Der Leser kann seine Helligkeit – z.B. um nachts nicht zu hell zu strahlen – der Helligkeit der Umgebung anpassen. Wenn diese Funktion gewünscht ist, aktivieren Sie den Umgebungslichtsensor.

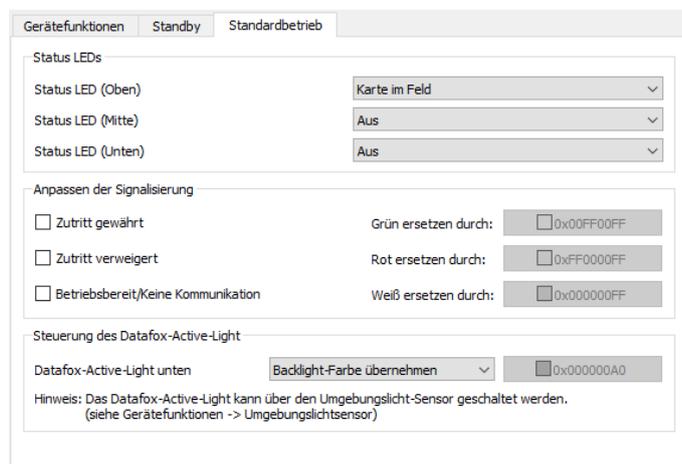
## Einstellung des Standby-Betriebs



Der Standby-Betrieb des EVO Intera II wird aktiviert, wenn der Näherungssensor für eine einstellbare Dauer keine Person in der Nähe erkannt hat. In diesem Betriebsmodus können den 3 LEDs vom normalen Betriebsmodus abweichende Funktionen zugewiesen werden.

Ferner kann – falls im Leser eingebaut – das Datafox-Active-Light geschaltet werden.

## Einstellung des Standardbetrieb

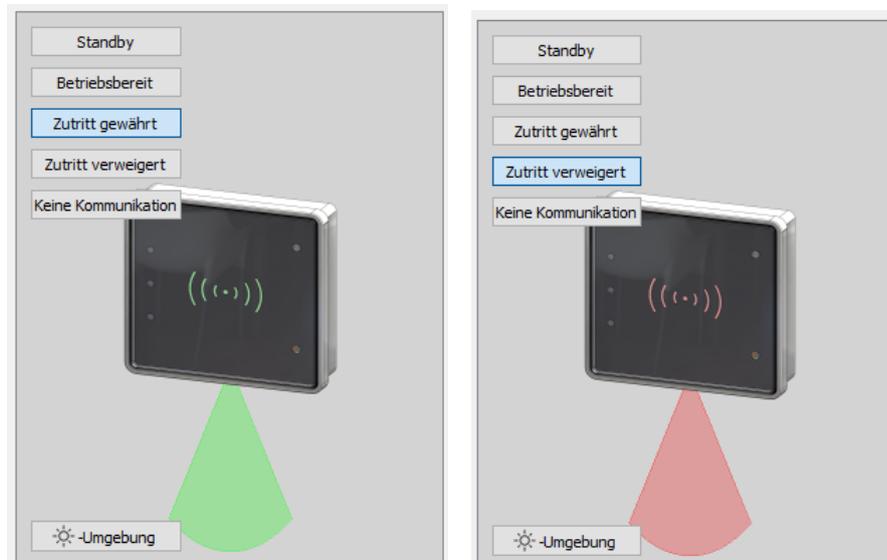


Im Standardbetrieb erfüllt der EVO Intera II die normalen Funktionen eines Zutrittslesers - der Leser über den Zutrittsbus durch einen Zutrittscontroller gesteuert. Im einfachsten Fall übermittelt der Leser die gelesenen RFID Daten an den Zutrittscontroller und wird dann auf Zutritt gewährt („Grün“) oder Zutritt abgewiesen („Rot“) geschaltet. Ist keine Zutrittssignalisierung aktiv, so leuchtet der Leser normalerweise weiß.

Sie können – neben der Funktionszuordnung der drei programmierbaren LEDs – die Farben, die für Grün, Rot und Weiß eingesetzt werden, anpassen. Ferner können Sie – falls im Gerät eingebaut – die Farbe und die Helligkeit des Datafox Active-Light einstellen.

## Vorschau des Leserverhaltens

Auf der rechten Seite der Konfigurationsmaske ist ein EVO Intera II dargestellt. Dieser ändert – bezogen auf die aktuell geladene Konfiguration – sein Aussehen. Den darzustellenden Betriebszustand wählen Sie über eine der fünf Schaltflächen aus.

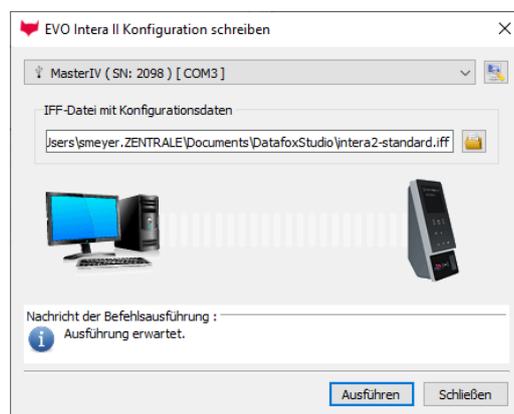


„Zutritt gewährt“ und „Zutritt verweigert“ mit Datafox Active-Light im Modus „Backlight-Farbe übernehmen“

Die Schaltfläche unten links im Vorschaubereich können Sie nutzen, um den Leser explizit in den Tag- bzw. Nacht-Betriebszustand zu versetzen.

## Übertragung zum / vom Gerät

Zur Übertragung auf oder von einem Leser schließen Sie diesen bitte über USB an Ihren PC an. Nach dem Betätigen einer der Schaltflächen zum Übertragen sehen Sie den Datei-Übertragungsdialog des Datafox Studios:



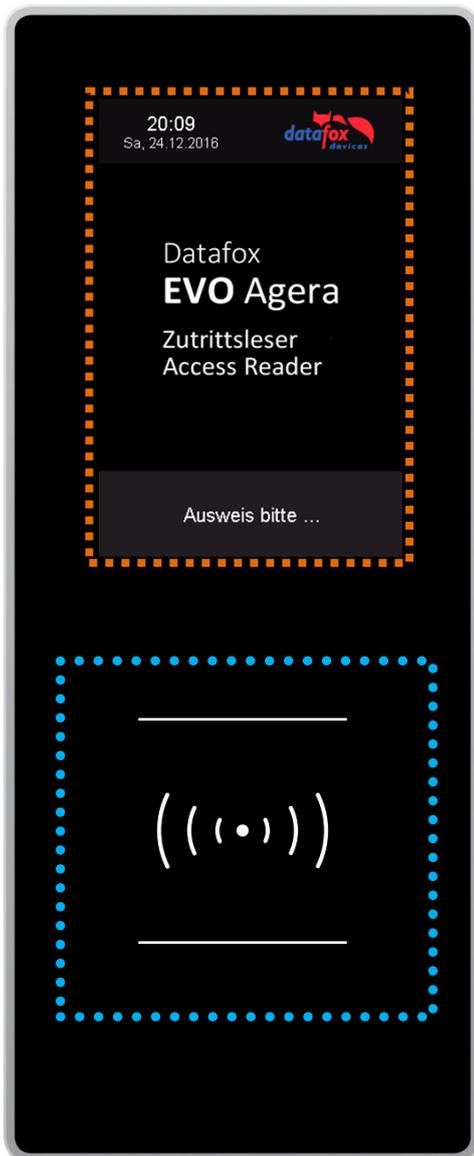
Hier können Sie die zu übermittelnde Konfigurationsdatei auswählen – die im Editor geöffnete Fassung ist über den Übertragungs-Button zum Gerät die Standard-Belegung des Übermittlungsdialogs. Durch das Betätigen der Schaltfläche „Ausführen“ wird die Konfigurationsdatei auf den Leser übermittelt (oder von dort gelesen).

### 3.5.6. Zutrittskontrolle II mit EVO Agera

#### 3.5.6.1. Aufbau der Anzeigen und Bedienung

Der Leser verfügt über einen kapazitiven Touch.

Alle dargestellten Bilder die vom Leser angezeigt werden und unten als Standard gekennzeichnet sind, können ausgetauscht werden.



Display:  
Das gesamte Displaybereich ist mit einem Touch hinterlegt.

Mit dem DatafoxStudioIV können hier Bilder für eine Galerieanzeige und für die notwendigen Ein / Ausgaben hinterlegt werden.  
Siehe → Konfiguration  
→ Displaydesigner.

• Lesebereich des Transponders mit Hintergrundbeleuchtung in RGB-Farben.  
• Die Steuerung der LED wird ausschließlich von der Firmware des Lesers gesteuert.

• Zutritt verweigert = **rot -**

• Zutritt gestattet = **grün -**

• Bios aktiviert = **blau -**

### 3.5.6.2. Anzeigen für den ZK-Status

Aktuell gibt es 2 Anzeigen für:

Zutritt gewährt:

Zutritt verweigert:



Datafox Standardbild



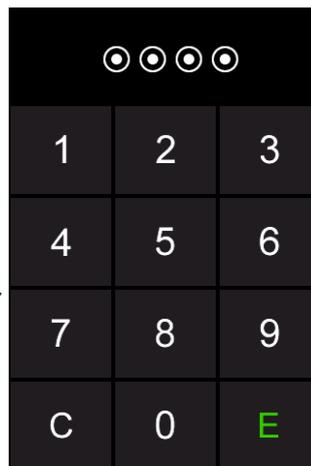
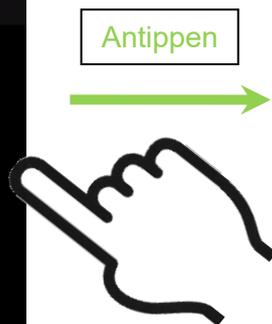
Datafox Standardbild

### 3.5.6.3. Anzeigen einer PIN-Tastatur

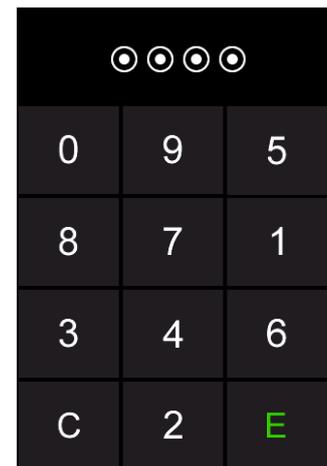
Wenn für den Zutritt noch eine zusätzliche PIN abgefragt wird, wird die Tastatur automatisch eingeblendet. Für den Zutritt nur über die Eingabe einer PIN genügt ein kurzes Antippen um die PIN-Anzeige zu aktivieren.



Datafox Standardbild  
Bild 1 der Galerie



Datafox Standardbild  
PIN normal



Datafox Standardbild  
PIN zufällige Anordnung

### 3.5.6.4. Fehlerausgaben

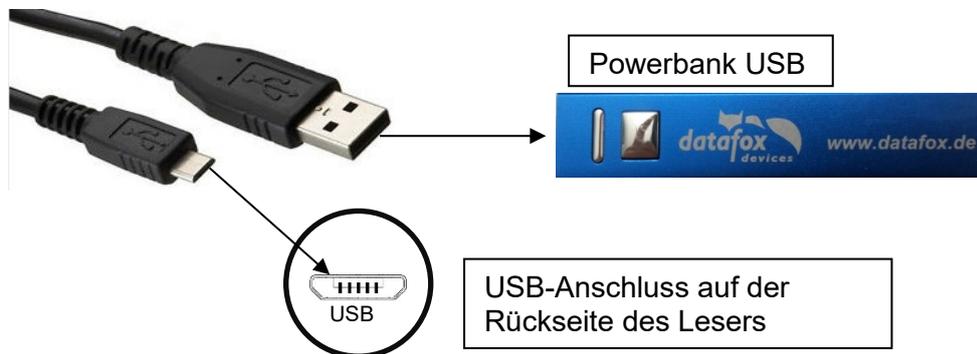
Der Leser steht in ständiger Kommunikation mit dem Master. Für den Fall das die Kommunikation unterbrochen wird, wird dies am Leser mit dem Text:Fehler Kommunikation.



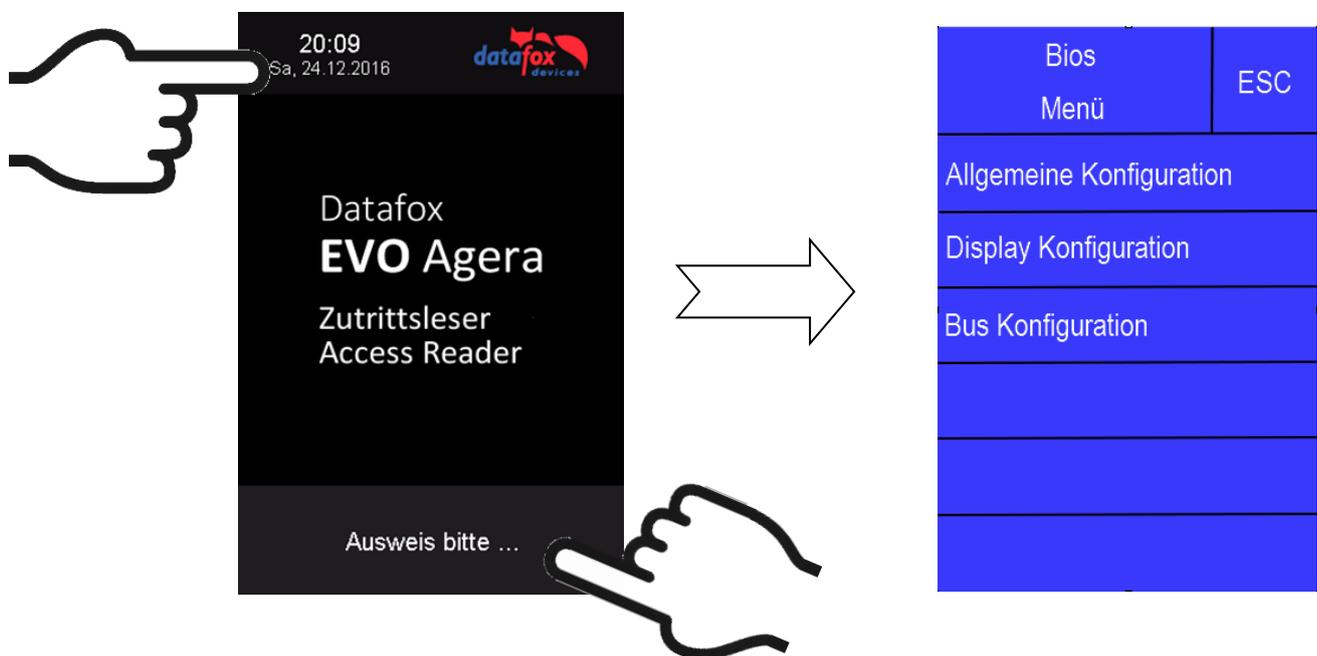
### 3.5.6.5. Bios-Menü

Schließen Sie den Leser mit dem Verbindungskabel an die 12V Spannungsversorgung an. Sobald dieser gestartet ist verbinden Sie den Leser per USB an einen PC oder auch einen kleinen Akku (Powerbank).

Nur wenn Spannung an dem USB-Anschluss anliegt, ist der Zugang zum Bios-Menü möglich.



Tippen Sie gleichzeitig links oben und rechts unten.



### 3.5.6.6. Allgemeine Konfiguration

In der Allgemeinen Konfiguration können folgende Informationen abgerufen werden:

- Installierte Firmware, Seriennummer
- Speicherbelegung für den Bilderspeicher
- Transpondertest für den Im Setup des Masters konfigurierten Transponder.

Allgemeine Konfiguration	ESC
Firmware Info	
Speicherbelegung	
Transpondertest	

### 3.5.6.7. Display Konfiguration

In der Display - Konfiguration kann folgendes parametrieren werden:

- die Helligkeit des Gerätes
- die Zufällige Nummerntasten – Anordnung bei der Pin – Tastatur
- die grundsätzliche Aktivierung der Pin – Tastatur

Display Konfiguration	ESC
Helligkeit	100%
Zufällige Tastenanordnung	Ein
Display TouchPin	Ein

### 3.5.6.8. Bus Konfiguration

In der Bus Konfiguration werden die Initialen Parameter, die zur Inbetriebnahme des Lesers gesetzt werden müssen, konfiguriert.

Bus Konfiguration	ESC
Bus Nummer	
Abschlusswiderstand	

### 3.5.6.9. Einstellen der Bus - Adresse

Die Bus – Adresse wird in der Bus Konfiguration unter "Bus Nummer" gesetzt.

Zu beachten ist, dass nur Bus – Adressen zwischen 1 und 16 möglich sind.

Die Eingabe der Bus – Nummer wird mit der "Enter" Taste (unten rechts) bestätigt.

Mit der Escape – Taste (unten links) kann der Vorgang abgebrochen werden.

Im Auslieferungszustand ist die Bus – Adresse 1 gesetzt.

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

### 3.5.6.10. Aktivierung des Bus - Abschlusswiderstands

Der Bus – Abschlusswiderstand von 120 Ω wird in der Bus Konfiguration unter "Abschlusswiderstand" entweder ein – oder ausgeschaltet.

Abschlusswiderstand	ESC
Ein	
Aus	

Hinweis: Handelt es sich um den letzten oder einzigen Leser im RS485 – Bus, so muss der Abschlusswiderstand eingeschaltet werden.

### 3.5.7. Funktionserweiterung für die Zutrittskontrolle 2

#### 3.5.7.1. Allgemeine Informationen

Die Zutrittskontrolle wurde um einige Funktionalitäten erweitert. Dazu wurde die Tabelle „**Action2**“ eingeführt. Diese ersetzt die bisher bekannte „**Action**“-Tabelle. Eine Beschreibung zum Aufbau der Tabelle „Action2“ finden Sie am Ende dieses Kapitels. Aufgrund der zusätzlichen Referenzen sind nun sehr viele Szenarien darstellbar.

Die nachfolgenden Beispiele geben einen kurzen Überblick dazu:

#### 3.5.7.2. Beispiele

##### Beispiel Werkstatt

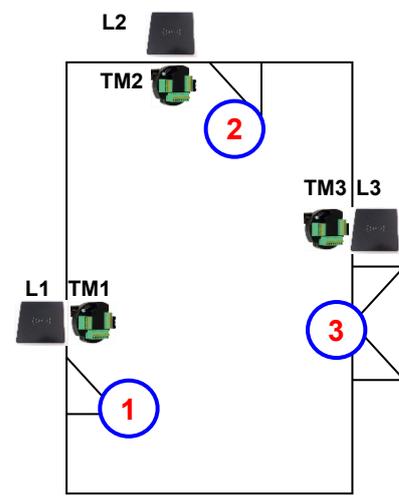
Der Hausmeister kommt am Morgen um 7.00 Uhr und nutzt dabei einen Eingang **1**.

> mit seinem Transponder wird der Eingang 1 für 5 Sekunden geöffnet.

> weiter wird das Tor **3** für das Öffnen mit einem Taster über einen Schließkontakt bis 16.00 Uhr (für 9 h) freigegeben, > und der Eingang **2** bleibt bis 16.00 Uhr (für 9h) für das Personal geöffnet.

Die Schließung erfolgt über:

- 1 - einen Transponder der Gruppe 40
- 2 - durch ein langes Vorhalten eines berechtigten Transponders an der jeweiligen Tür
- 3 - automatisch um 16.00 Uhr (muss im Zeitmodell hinterlegt werden siehe Nr.2 in Spalte „RefTime“)



Der Aufbau der Reader-, Location-, Action2- und Identification-Tabellen könnte wie folgt aussehen:

Tabelle Reader

ID	ZM	TM	RefLocation	RefAction	PinGeneral	Beschreibungstext
1	1	320	0	0	0	Mastergerät
2	1	010	100	0	0	Türmodul an RS485 (TM1) Da dies nur ein Türmodul ist, muss hier keine Action ausgeführt werden.
3	1	011	100	1000	0	Leser über RS232 (L1) Wird an diesem Leser eine Buchung getätigt, wird jede Action mit der ID 1000 ausgeführt.
4	1	020	200	0	0	Türmodul an RS485 (TM2) Da dies nur ein Türmodul ist, muss hier keine Action ausgeführt werden.
5	1	021	200	2000	0	Leser über RS232 (L2) Wird an diesem Leser eine Buchung getätigt, wird jede Action mit der ID 2000 ausgeführt.
6	1	030	300	0	0	Türmodul an RS485 (TM3) Da dies nur ein Türmodul ist, muss hier keine Action ausgeführt werden.
7	1	031	300	3000	0	Leser über RS232 (L3) Wird an diesem Leser eine Buchung getätigt, wird jede Action mit der ID 3000 ausgeführt.

### 3.5.7.3. Tabelle Time

ID	Weekdays	TimeStart	TimeEnd	Beschreibung
1	1234567	00:01	23:59	24h Buchungen möglich
2	1234567	07:00	16:00	Zeit für Daueröffnung
3	1234567	16:00	16:05	Zeitmodell für automatische Relaisabschaltung

Tabelle Action2

ID	RefGroup	RefTime	RefReader Relais	PortOut	Elapse	RefReader LED	RefTime Relais	Beschreibung
<b>Buchungen am Leser 1</b>								
1000	10	0	2	1	5	3	0	Normales Öffnen für 5s. Gruppen (10; 20; 30) haben Zugang. (immer)
1000	20	0	2	1	5	3	0	
1000	30	0	2	1	5	3	0	
1000	30	2	4	1	32400	5	0	Tür 2 wird für 9h geöffnet.
1000	30	2	6	1	32400	7	0	Tor 3 wird für 9h freigegeben.
1000	40	0	4	1	-1	3	0	Türöffnung wird mit Ausweis zurückgenommen.
1000	40	0	6	1	-1	5	0	Torfreigabe wird mit Ausweis zurückgenommen.
<b>Buchungen am Leser 2</b>								
2000	10	0	4	1	5	5	0	Normales Öffnen für 5s. Gruppen (10; 20; 30) haben (immer)
2000	20	0	4	1	5	5	0	
2000	30	0	4	1	5	5	0	
2000	30	2	4	1	32400	5	0	Tür 2 wird bis 16Uhr geöffnet.
2000	30	2	6	1	32400	7	0	Tor 3 wird für 16Uhr freigegeben.
2000	40	0	4	1	-1	5	0	Türöffnung wird mit berechtigtem Ausweis zurückgenommen.
2000	40	0	6	1	-1	7	0	Torfreigabe wird mit berechtigtem Ausweis zurückgenommen.
2000	0	0	4	1	-1	5	3	Türöffnung wird automatisch um 16:00 Uhr über Zeitmodell zurück genommen.
2000	0	0	6	1	-1	7	3	Türöffnung wird automatisch um 16:00 Uhr über Zeitmodell zurück genommen.
<b>Buchungen am Tor (Leser 3)</b>								
3000	0	0	6	1	5	0	0	Für alle Gruppen die in der Location für das Tor (L3) eingetragen sind, wird diese Action ausgeführt.

Tabelle Location

ID	refGroup	refTime	refTimeNoPin	Bemerkungen
100	10	1	0	Gruppe 10, 20, 30 und 40 haben Zutritt an diesem Leser.
100	20	1	0	
100	30	1	0	
100	40	1	0	
200	10	1	0	Gruppe 20 kann den Eingang L2 nicht benutzen.
200	30	1	0	
200	40	1	0	
300	10	1	0	Nur der Werkstattleiter und der Hausmeister können das Tor öffnen. Der Hausmeister ist aber nicht berechtigt, die Daueröffnung von hier aus zu aktivieren.
300	30	1	0	

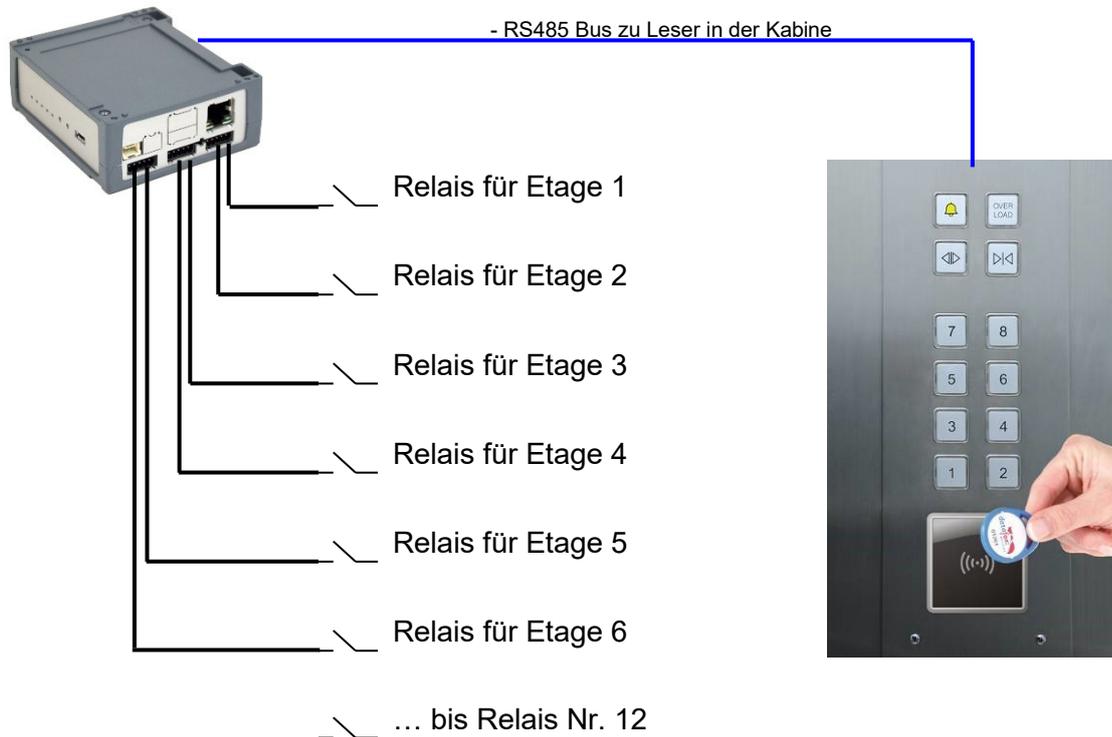
Tabelle *Identification*

ID	Group	Pin	Menace	ActiveStart	ActiveEnd	Active	Beschreibung
1111	10	0	0	2005-01-01	2099-12-31	1	Werkstatteleiter
2222	20	0	0	2005-01-01	2099-12-31	1	Angestellte
3333	30	0	0	2005-01-01	2099-12-31	1	Hausmeister
4444	40	0	0	2005-01-01	2099-12-31	1	Hausmeister 2, Transponder für Schließung

### Beispiel Aufzugsteuerung

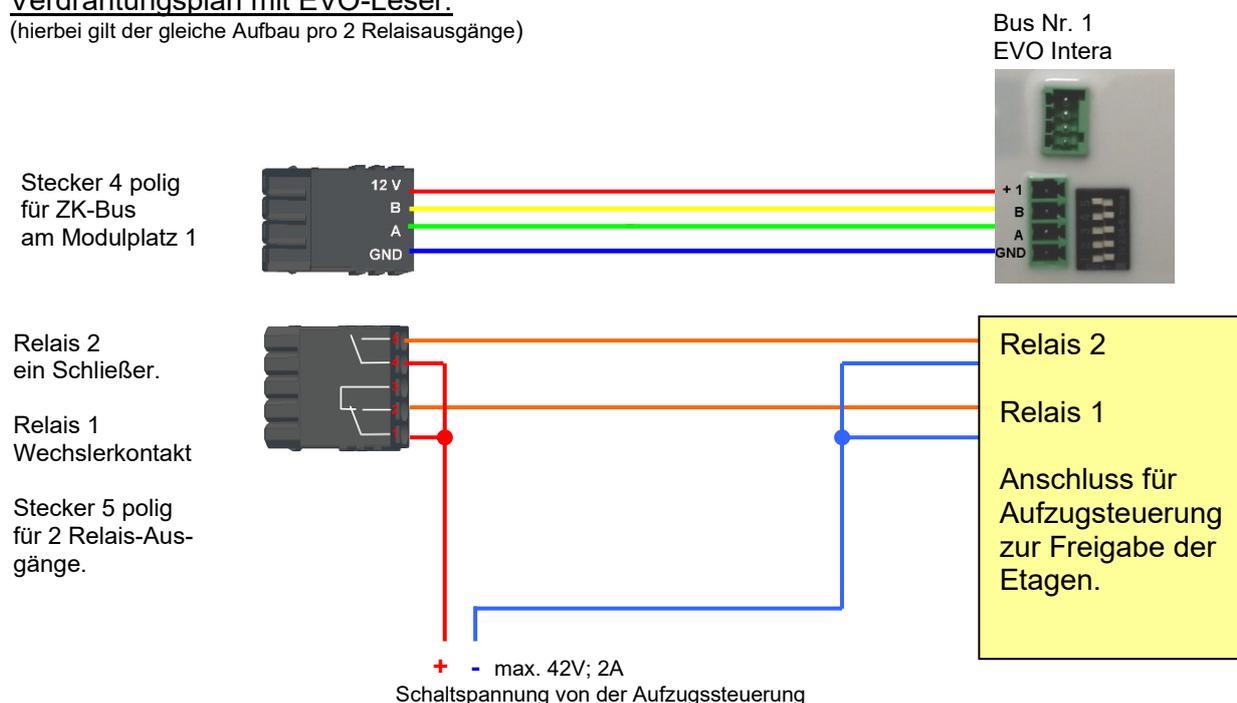
Ziel ist es, das die jeweiligen Mieter nur in ihre Etage fahren dürfen. Hält der Mieter seinen Transponder vor, so wird der Taster am Bedienfeld im Fahrstuhl für die Etage, in der der Mieter wohnt, für 20 Sekunden freigegeben.

In der Aufzugskabine ist ein Transponderleser angebracht und die Steuerung (KYO Cenloc) befindet sich auf der Kabine.



### Verdrahtungsplan mit EVO-Leser:

(hierbei gilt der gleiche Aufbau pro 2 Relaisausgänge)



Der Aufbau der Reader-, Location-, Action2- und Identification- Tabellen könnte folgendermaßen aussehen:

Tabelle Reader

ID	ZM	TM	RefLocation	RefAction	PinGeneral	Beschreibungstext
1	1	320	0	0	0	Mastergerät
2	1	000	100	1000	0	Leser an RS485

Tabelle Action2

ID	RefGroup	RefTime	RefReader Relais	PortOut	Elapse	RefReader LED	RefTime Relais	Beschreibung
Buchungen am Leser in der Kabine								
1000	10	0	1	1	20	2	0	Gruppe 10 für Etage 1.
1000	20	0	1	2	20	2	0	Gruppe 20 für Etage 2.
1000	30	0	1	3	20	2	0	Gruppe 30 für Etage 3.
1000	40	0	1	4	20	2	0	Gruppe 40 für Etage 4.
1000	50	0	1	5	20	2	0	Gruppe 50 für Etage 5.
1000	60	0	1	6	20	2	0	Gruppe 60 für Etage 6.
1000	102	0	1	1	20	2	0	Gruppe 102 darf in die Etagen 1 und 2 fahren.
1000	102	0	1	2	20	2	0	
1000	104	0	1	1	20	2	0	Gruppe 104 darf in die Etagen 1,2 und 3 fahren.
1000	104	0	1	2	20	2	0	
1000	104	0	1	3	20	2	0	

Tabelle Location

ID	refGroup	refTime	refTimeNoPin	Bemerkungen
100	10	1	0	Die Gruppen 10, 20, 30, 40, 50, 60,102 und 104 müssen am Leser (Raum) zugelassen sein.
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	

Tabelle Identification

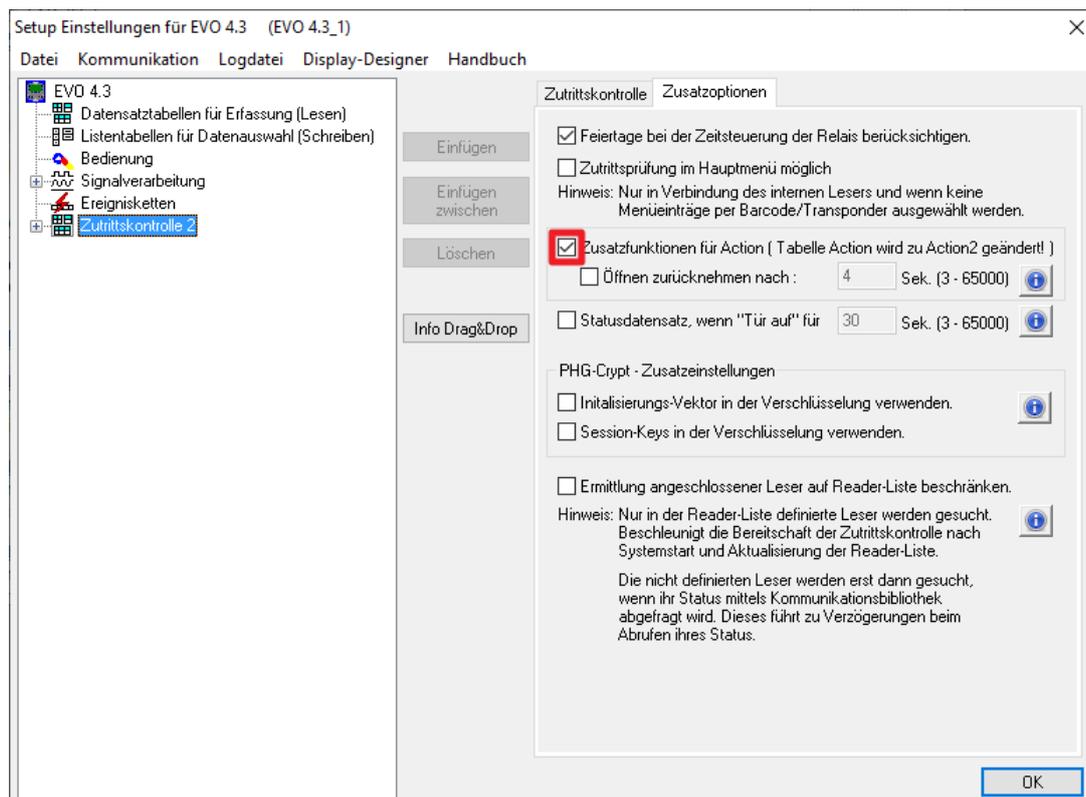
ID	Group	Pin	Menace	ActiveStart	ActiveEnd	Active	Beschreibung
1111	10	0	0	2005-01-01	2099-12-31	1	Mieter Wohnung 1. Etage
2222	20	0	0	2005-01-01	2099-12-31	1	Mieter Wohnung 2. Etage
3333	30	0	0	2005-01-01	2099-12-31	1	Mieter Wohnung 3. Etage
4444	40	0	0	2005-01-01	2099-12-31	1	Mieter Wohnung 4. Etage
5555	50	0	0	2005-01-01	2099-12-31	1	Mieter Wohnung 5. Etage
6666	60	0	0	2005-01-01	2099-12-31	1	Mieter Wohnung 6. Etage
1102	102	0	0	2005-01-01	2099-12-31	1	Etage 1 und 2 erlaubt
1104	104	0	0	2005-01-01	2099-12-31	1	Etage 1, 2 und 3 erlaubt

Tabelle Time

ID	Weekdays	TimeStart	TimeEnd	Beschreibung
1	1234567	00:01	23:59	24h gültig an 7 Tage in der Woche

### 3.5.7.4. Beschreibung der Tabelle „Action2“

Das Umschalten der Tabelle „Action“ in „Action2“ erfolgt im DatafoxStudioIV.



Bezeichner	Datentyp	Länge	Beschreibung
ID	Nummer (int)	4	Enthält eine eindeutige ID. Sind mehrere gleiche IDs vergeben, werden alle Aktionen mit ID ausgeführt.
RefGroup	Nummer (int)	4	Verweist auf die Gruppe für die diese Aktion durchgeführt werden darf. 0 = Alle Gruppen, die in der Location zugelassen sind, führen diese Action aus.
RefTime	Nummer (int)	4	Verweist auf den Zeitraum, an der die Aktion durchgeführt werden darf. (0 = immer gültig) <b>! Nicht mit Zeitangaben in RefTimeRelais vermischen!</b>
RefReader Relais	Nummer (int)	4	Verweist auf die Reader Tabelle und gibt an, an welchem Modul oder Master das Relais geschaltet wird.
PortOut	Nummer (char)	1	Gibt an, welcher Relaisausgang geschaltet wird. Mögliche Angaben: 1 -9 und A-W, entspricht Port 1-32 (digital out)
Elapse	Nummer (txt)	6	Gibt die Zeit an, wie lange ein Relais geschaltet wird. <b>! Die Angabe erfolgt hier in Sekunden!</b> Ist hier (-1) eingetragen, werden die Relaisschaltungen sofort zurückgenommen Ist hier (0) eingetragen, so werden die Relais für den unter RefTime angegebenen Zeitraum ab der Buchung geöffnet. "FRA" activates Free Access = Freier Zutritt an diesem Leser "BLA" activates Blocked Access = Leser gesperrt. Dauerrot am Leser "STD" returns to Standard mode.= Deaktivieren von FRA bzw.. BLA
RefReaderLED	Nummer (int)	4	Verweist auf die Reader Tabelle und gibt an, an welchem Modul zusätzlich die grüne LED parallel zum Relais geschaltet wird.
RefTimeRelais (nur für Automatische Zeitsteuerung)	Nummer (int)	4	Das Zeitmodell gibt an, wann der Ausgang dauerhaft geschaltet wird. (0 = wird nicht verwendet). Wird ein Zeitmodell angegeben, so wird diese Aktion zur angegebenen Zeit durchgeführt. (Automatische Zeitsteuerung) Bei einer Zeitangabe ( 1 1234567 00:00-23:59) ist der Ausgang 24h 7 Tage eingeschaltet. <b>! Aktionen die hier ausgeführt werden, dürfen nicht mit Zutrittsaktionen gemischt werden!</b>

**Achtung:**  
 Durch Übertragen der Tabelle „Action2“ an das Gerät, wird die Tabelle „Action“ ersetzt.  
 Somit werden nur noch Einträge der Tabelle „Action2“ berücksichtigt.

**Achtung:**  
 Möchten Sie weiterhin nur mit der „Action“ Tabelle arbeiten, so darf die Tabelle „Action2“ nicht an das Gerät übertragen werden.  
 Wurde bereits eine Tabelle „Action2“ an das Gerät übertragen, muss diese durch das Einspielen eines Setups gelöscht werden.

### 3.5.7.5. Weitere Funktionen für ZK

Alle nachfolgenden beschriebenen Funktionen werden nur im Zusammenhang mit der **Action 2** Tabelle unterstützt.

Mögliche Funktionen:

- Protokollieren, in einer internen Liste, in welchem Raum sich welcher Mitarbeiter befindet.
- Hard antipassback
- Soft antipassback (= es wird nur der Software mitgeteilt, dass ein Ausweis 2 mal in einen Raum betreten hat = Statusmeldung 251)
- EMA (Alarmanlage schalten)
- Automatische Relaisabschaltung nach Öffnung der Tür

Die Tabelle „**ReaderProps**“ muss unter der Tabellenstruktur der Bedienung angelegt werden:

Name	Data type	Length	Description
RefReader	Number (int)	4	Referenz auf die Reader Liste hier wird der Leser angegeben bei dem die Funktion angewendet wird.
Type	Number (int)	2	Type of the Property 0 = no additional functionality = keine Sonderfunktion aktiv 1 = anti-passback = antipassback aktiviert 2 = EMA-Steuerung 3 = EMA 4 = EMA 5 = Türüberwachung -> Relais aus nach Tür-Öffnung
Mode	Number (int)	1	Funktion <b>Antipassback:</b> 1 – Protokollfunktion es wird ein Eintrag in der Liste ("presence" erstellt). Diese Liste kann dann per Software ausgelesen werden. 2 – Hard anti-passback (kein Zutritt gewährt, status code 250, erst nach Ablauf der Zeit Duration oder wenn der Zutritt in einem anderem Raum gebucht wird.) 3 – Soft anti-passback (Zutritt wird gewährt, und Status code 251).
Duration	Number (int)	10	Zutritt wird nach Ablauf der Duration Zeit wieder erlaubt. Wert in Sekunden. 0 = Keine Ablaufzeit. Es muss zwingend der Zutritt zu einem anderen beliebigen Raum erfolgen.

Die Tabelle „**ReaderProps**“ im Setup angelegt:

### Protokoll - Funktion

Dient im Wesentlichen dazu, dass bei der Verwendung von mehreren Zutrittsmanagern dieser weiß, in welchem Raum sich eine Person befindet.

Über Ihre Software, wird diese Information zwischen den Zutrittsmanagern verteilt oder kann bei Bedarf auch ausgelesen werden.

Siehe hierzu Dokumentation DFComDLL

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

## Soft antipassback

Hier wird eine Statusmeldung 251 ausgegeben, wenn ein und der Selbe Ausweis mehr als einmal den gleichen Raum betritt. Der Zutritt wird trotzdem zugelassen!

## Hard antipassback

Ein Leser ist immer einem Raum zugeordnet. Dieser Raum darf dann mit demselben Ausweis nur einmal betreten werden. Wird der Selbe Ausweis noch einmal für den Zutritt in diesem Raum genutzt, wird dieser abgewiesen. Der Status 250 wird bei der ZK im Datensatz ausgegeben.

Hier können Sie wählen, ob das Abweisen Zeitlich begrenzt wird, oder Hard aktiv bleibt.

Für den Fall Hard-Aktiv wird der Zutritt erst wieder erlaubt, wenn der Zutritt in eine andere Raum ID erfolgt ist. Dies entspricht dann dem Verlassen des Vorhergehenden Raumes.

### 3.5.7.6. Liste Presence

Diese Liste wird vom ZK-Kontroller selbst angelegt.

Hiermit ist es möglich, eine Personen-Raumverfolgung über mehrere ZK-Kontroller zu ermöglichen. Soll die Funktion Antipassback über mehrere ZK-Kontroller genutzt werden, muss diese Liste immer durch die Software an alle ZK-Kontroller aktualisiert werden.

#### Beispiel:

Ein Raum (Beispiel Raum-ID 10) hat mehrere Türen die von unterschiedlichen ZK-Boxen verwaltet werden.

Tritt nun eine Person in diesen Raum, so wird in der Presence-Liste an dieser Box ein Eintrag erstellt, dass diese Person sich im Raum befindet.

Die anderen ZK-Boxen, können nun ebenfalls darüber informiert werden, dass sich die Person mit der ID X im Raum 10 befindet.

Dazu muss über Ihre Software (mit DLL) in den anderen Boxen ein Eintrag in der Liste Presence erstellt werden.

Dies erfolgt über die Methode [DFCTableAppendRowData](#) Datenzeile an die Tabelle anfügen.

Gleiches gilt, wenn eine Person den Raum verlässt, muss dieser Eintrag in den Anderen ZK-Boxen gelöscht werden.

Name	Datentyp	Länge	Beschreibung
ID	Number (int)	20	ID der Person die den Raum betreten hat. Die ID Identification.
RefLocation	Number (int)	4	Referens zur Raumliste Location.
TimeStamp	Number (int)	10	Zeitstempel, wann die Person den aktuellen Raum betrat Integer Wert in Sekunden. -> Sekunden Wert ab dem 01.01.2000 00:00Uhr

### 3.5.8. Anbindung EMA (Einbruchmeldeanlage)

Ab der Firmware-Version 04.03.12 ist es möglich, eine Einbruchmeldeanlage (EMA) in die Zutrittskontrolle zu integrieren.

Mit PIN-Zutrittslesern ist es möglich, bis zu fünf Alarmbereiche einer Einbruchmeldeanlage scharf bzw. unscharf zu schalten.

Die Scharfschaltung eines EMA-Bereiches hat zur Folge, dass sämtliche Zutrittsbuchungen, die in diesem Bereich durchgeführt werden, abgewiesen werden. Zutrittsbuchungen werden nach der üblichen Prüfung der diversen Zutrittsregelungen nur dann zugelassen, wenn der entsprechende Leser keinem EMA-Bereich zugeordnet oder dieser Bereich nicht scharf geschaltet ist. Bei Abweisung wird ein entsprechender Buchungssatz mit „EMA scharf“ erzeugt.

Scharf- und Unscharfschaltung sind unter Berücksichtigung der konfigurierten Regeln an den entsprechend zugeordneten PIN-Zutrittslesern jederzeit möglich.

Ein zweiter Versuch, einen Bereich scharf oder unscharf zu schalten, wird, ebenfalls mit einem entsprechenden Buchungssatz „EMA bereits scharf“ bzw. „EMA bereits unscharf“, zugelassen.

#### 3.5.8.1. Konfigurieren der EMA in der Zutrittskontrolle

Zur Aktivierung der EMA in der Zutrittskontrolle wird die Setup-Liste „ReaderProps“ benötigt. Bisher wurde über diese Liste ausschließlich das „AntiPassBack“ konfiguriert. Zwölf Spalten werden in dieser Liste zur Einrichtung der EMA benötigt.

##### **Hinweise:**



Falls die Listen mit dem DatafoxStudioIV übertragen werden sollen, ist es nicht möglich, „leere“ Spalten zu übertragen. Füllen Sie dann bitte Felder, die leer bleiben sollen, mit einer „0“.

Die Spaltenbreiten in der „ReaderProps“-Liste können Sie beliebig vorgeben. Wichtig ist nur, dass die gewünschten Informationen vollständig in die einzelnen Spalten passen!

Zur Konfiguration werden drei Typen von Einträgen benötigt. Zum einen werden die/das Relais und der/die digitalen Eingänge zur Steuerung und Statusabfrage der EMA konfiguriert. Weiterhin werden die PIN-Leser und die Codes zur Aktivierung/Deaktivierung definiert. Letztlich werden die Leser den einzelnen Alarmbereichen zugeordnet.

Die Reihenfolge der Einträge in der „ReaderProps“ Liste spielt dabei keine Rolle.

### 3.5.8.2. Relais und digitale Eingänge zur Steuerung (Type 2)

Hier wird in der ReaderProbs konfiguriert, ob und welche Relais zum Scharf-/ Unscharfschalten eines Alarmkreises benutzt werden. Ebenso ob und welcher digitale Eingang die Bereitschaft der EMA zur Scharfschaltung anzeigt und mit welchem digitalen Eingang die Scharfschaltung zurückgemeldet wird.

Spalte	Name im Setup	Data type	Length	Description
1	RefReader	Number (int)	4	Wird für die EMA Type=2 Steuerung nicht benötigt, kann leer bleiben. Für AntiPassBack muss der Leser angegeben werden.
2	Type	Number (int)	variable 10	2 = EMA – Steuerung: Definition der Din und Relais
3	Area	Number (int)	variabel max. 10	Nummer des zugeordneten EMA-Bereiches
4	OutArmReader	Number (int)	4	Referenz auf die Reader-Liste welcher Ausgang geschaltet werden soll. Gilt für die Scharfschaltung.
5	OutArmPort	1-9; A...	1	Nummer den Ausgangs
6	OutUnarmReader	Number (int)	4	Referenz auf die Reader-Liste welcher Ausgang geschaltet werden soll. Gilt für die UnScharfschaltung.
7	OutUnarmPort	1-9; A...	1	Nummer den Ausgangs
8	InRdyReader	Number (int)	4	Referenz auf die Reader-Liste welcher Eingang signalisiert, wenn die EMA bereit ist zum Scharfschalten.
9	InRdyPort	1-9; A...	1	Nummer den Eingangs
10	InArmedReader	Number (int)	4	Referenz auf die Reader-Liste welcher Eingang signalisiert, wenn die EMA Scharf geschaltet ist.
11	InArmedPort	1-9; A...	1	Nummer des Eingangs des in Spalte 10 referenzierten Geräts
12	OutElapse	Number (int)	4	0 → das Schaltrelais für die EMA-Aktivierung / EMA-Deaktivierung zieht dauerhaft an, sonst gibt es nur einen Impuls mit X Sekunden Dauer.

Beschreibung ReaderProbs für (Type=2) Ein- und Ausgänge Definition!

#### Hinweise:



Falls das Scharf-/ Unscharfschalten über dasselbe Relais erfolgen soll, müssen die Spalten OutUnarmReader und OutUnarmPort die gleichen Werte enthalten wie OutArmReader und OutArmPort. Das geschaltete Relais bedeutet dann: „Scharfschalten“, das Relais im Ruhezustand: „Unscharfschalten“.

Falls keine Referenz „InRdyRead“ angegeben wird, ist die EMA jederzeit bereit, um scharf geschaltet zu werden.

### 3.5.8.3. Definition der Codes zum Ein- und Ausschalten (Type 3)

Um an einem PIN-Leser einen Alarmbereich ein-/ und ausschalten zu können, wird folgender Eintrag benötigt.

Spalte	Name im Setup	Data type	Length	Description
1	RefReader	Number (int)	4	Referenz (ID) auf den PIN-Leser in der Reader-Liste.
2	Type	Number (int)	variabel max. 10	3 = EMA – Steuerung: PIN-Code zum Scharf und Unscharf schalten
3	Area	Number (int)	variabel max. 10	Nummer des zugeordneten EMA-Bereiches
4	CodeOn	Number (int)	2	Bei Eingabe dieser Ziffernfolge am Leser soll scharf geschaltet werden. Es sind maximal zwei Ziffern zulässig. PIN zur Scharfschaltung
5	CodeOff	Number (int)	2	Bei Eingabe dieser Ziffernfolge am Leser soll unscharf geschaltet werden. Maximal sind zwei Ziffern zulässig. PIN zur UnScharfschaltung.
6	RefGroup	Number (int)	4	Um die Schaltung zu legitimieren, muss der Ausweis dieser Gruppe zugeordnet sein. Mit dem Wert „0“ ist jeder „EMA-berechtigte“ Ausweis für diese Schaltung zugelassen.
7	Keine Angaben notwendig.			
8				
9				
10				
11				
12				

#### Hinweise:

Falls an einem Leser mehrere Alarmkreise geschaltet werden sollen, benötigt jeder Kreis einen eigenen Eintrag.



Auch eine einzelne Null ,0', Vornull ,0x' oder auch eine Doppelnull ,00' sind hier als jeweils eigener Schaltcode zulässig!

Falls ein Kreis nur ein- oder nur ausgeschaltet werden soll, tragen Sie in das andere Schaltcodefeld ein Minus ,-' ein, da ,0' einen gültigen Code darstellen würde!

Achten Sie darauf, keinen Schaltcode doppelt zu vergeben, da das Verhalten der Anlage sonst ungewiss ist.

### 3.5.8.4. Zuordnung der Leser zu EMA-Bereichen (Type 4)

Damit bei scharf geschaltetem Alarmkreis Buchungen an Lesern abgewiesen werden können, müssen die Leser den vorhandenen Alarmkreisen zugeordnet werden.

Spalte	Name im Setup	Data type	Length	Description
1	RefReader	Number (int)	4	Referenz (ID) auf die Leser-Definition in der Reader-Liste
2	Type	Number (int)	variabel max. 10	4 = EMA – Steuerung: Zuordnung der EMA-Bereiche
3	Area	Number (int)	variabel max. 10	Nummer des zugeordneten EMA-Bereiches
4	Keine Angaben notwendig.			
5				
6				
7				
8				
9				
10				
11				
12				

#### Hinweise:



Ein Leser darf sich auch in mehreren Alarmkreisen befinden. Für jeden Kreis wird dann ein eigener Eintrag in der Liste ReaderProps benötigt.  
An Lesern, die keinem Alarmkreis zugeordnet sind, kann jederzeit unter Berücksichtigung der restlichen ZK ‚normal‘ gebucht werden.

### 3.5.8.5. Ausweise zur EMA-Schaltung berechtigen

Um mit einem Ausweis eine EMA-Schaltung durchzuführen, ist es notwendig, diesen in der Identification-Tabelle anzulegen. Die entsprechende Gruppe (s. Kapitel 3.5.8.3, Spalte 6 „Group“) muss in der Spalte „Group“ eingetragen sein. Der Wert der Spalte „ActiveGeneral“ muss auf „7“ gesetzt sein. Mit dem Wert „0“ in der Spalte „Group“, ist der Ausweis berechtigt, jede EMA-Schaltungen durchzuführen, auch dann, falls für das Ein-/ Ausschalten eine Gruppe hinterlegt ist (s. 3.5.8.3, Spalte 6). Wird ein konfigurierter Schaltcode + ‚E‘ an einem PIN-Leser eingegeben, beginnt der Leser im Wechsel rot und grün zu blinken. Innerhalb der Timeout-Zeit (5 Sekunden) muss daraufhin ein für die EMA-Schaltung gültiger Ausweis zur Legitimation vorgehalten werden. Je nach Status wird dann die EMA-Buchung mit „grün“ zugelassen oder „dreimal rot“ abgewiesen.

Beispiel für die Identification Tabelle:

Der Ausweis 59780 kann sowohl die EMA scharf- und unscharf schalten als auch ‚normal‘ Zutritt an den Türen bekommen.

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

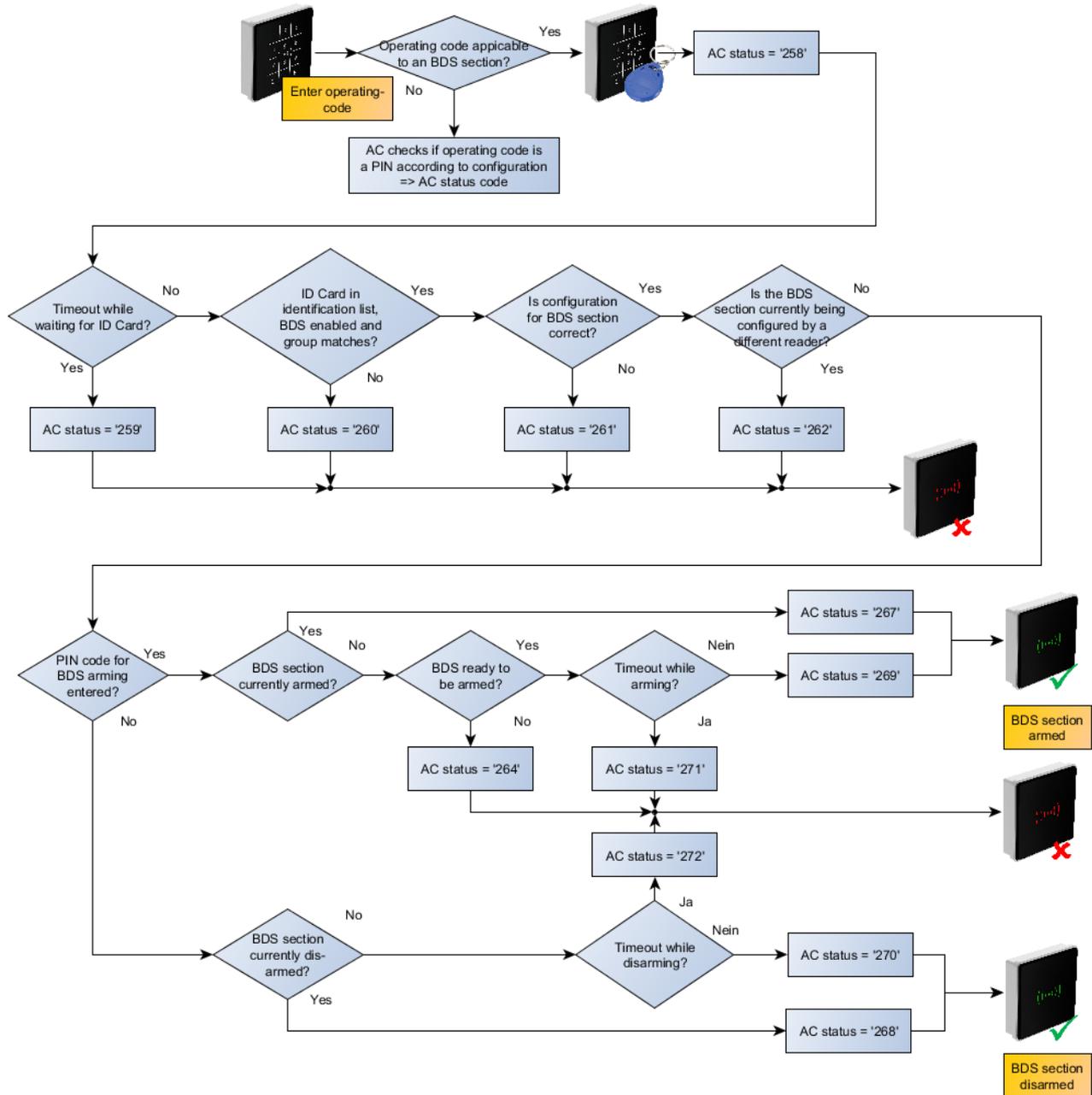
### 3.5.8.6. Statuscodes

Die folgenden Statuscodes sind in der ZK für die Einbindung der EMA neu aufgenommen worden, um den Status der Anlage nach außen dokumentieren zu können:

EMA	Beschreibung
258 <sup>1</sup>	Nach einer EMA-Buchung an einem entsprechend konfigurierten PIN-Leser wird auf die Identifizierung (Transponder + ggf. Pin) gewartet.
259	Nach einer EMA-Buchung wurde nicht innerhalb von fünf Sekunden ein Ausweis vor den Leser gehalten, um die Buchung zu legitimieren.
260	Der vorgehaltene Ausweis zur Legitimation der EMA-Buchung ist nicht zugelassen. Entweder ist die Ausweisnummer unbekannt, der Ausweis ist in der Identification-Tabelle nicht für EMA-Schaltungen freigeschaltet oder die Gruppe hat keine EMA-Schaltberechtigung. (ActiveGeneral <b>nicht</b> auf 7)
261	Der eingegebene EMA-Bereich ist nicht richtig konfiguriert worden.
262	Während einer Scharf- oder Unscharfschaltung eines EMA-Bereiches ist für diesen Bereich keine weitere EMA-Aktion möglich.
263 <sup>1</sup>	Die EMA meldet per digitalem Eingang, dass sie zur Scharfschaltung bereit ist.
264 <sup>1</sup>	Die EMA meldet per digitalem Eingang, dass sie nicht zur Scharfschaltung bereit ist.
265	Per Steuersignal (Relais) wird einem EMA-Bereich mitgeteilt, dass er scharf schalten soll.
266	Per Steuersignal (Relais) wird einem EMA-Bereich mitgeteilt, dass er unscharf schalten soll.
267	Der scharf zu schaltende EMA-Bereich ist bereits scharf geschaltet. Am Leser wird dennoch „grün“ signalisiert, damit der Benutzer erkennt, dass die EMA scharf ist.
268	Der unscharf zu schaltende EMA-Bereich ist bereits unscharf geschaltet. Am Leser wird dennoch „grün“ signalisiert, damit der Benutzer erkennt, dass die EMA unscharf ist.
269 <sup>1</sup>	Der EMA-Bereich ist jetzt scharf.
270 <sup>1</sup>	Der EMA-Bereich ist jetzt unscharf.
271	Der EMA-Bereich konnte innerhalb von fünf Sekunden nicht scharf geschaltet werden. Der zugeordnete digitale Eingang meldet nach wie vor ‚unscharf‘.
272	Der EMA-Bereich konnte innerhalb von fünf Sekunden nicht unscharf geschaltet werden. Der zugeordnete digitale Eingang meldet nach wie vor ‚scharf‘.
273	Die Zutrittsbuchung wird wegen eines scharf geschalteten EMA-Bereiches abgewiesen.
274	Bei der Identifizierung wird zusätzlich eine PIN benötigt.
275	Die eingegebene PIN passt nicht zu der hinterlegten.
276	Die eingegebene PIN passt zu der hinterlegten.
277	Timeout bei der Pin-Eingabe

<sup>1</sup>) Bei diesen Statuscodes wird im Feld „Ausweisnummer“ der jeweilige EMA-Bereich [1..5] angegeben.

### 3.5.8.7. Aktivierungsablauf im Controller



## Beispiel zur EMA-Einbindung

Es folgen nun Beispieltabellen, wie eine einfache EMA-Konfiguration aussehen könnte:

Es wird der EMA-Bereich „2“ aktiviert. Mit dem 3. Relais des Zutrittscontrollers wird die Scharfschaltung angefordert, mit dem 4. Relais, die Unscharfschaltung. Der Eingang 1 am Controller zeigt an, ob die EMA zur Scharfschaltung bereit ist oder nicht. Der Eingang 2 gibt den Status hinsichtlich der Scharfschaltung wieder.

Mit dem Code „11+E“ kann die EMA scharfgeschaltet werden, mit dem Code „22+E“ unsharp. Berechnigte Ausweise müssen der Gruppe „8“ zugeordnet sein.

In der Anlage sind die beiden Leser mit den IDs „104“ und „105“ der EMA zugeordnet, so dass hier nur dann ‚normal‘ gebucht werden kann, wenn die EMA unsharp geschaltet ist.

## Beispiel ReaderProps-Tabelle

;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-Tabelle

In der Reader-Tabelle ist neben den beiden Lesern der Anlage auch der Controller „999“ aufgeführt.

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

In der Action2-Tabelle sind für die Öffnung der beiden Türen die Relais 1 und 2 des Controllers referenziert – diese Einstellung ist nicht für den EMA Abschnitt erforderlich.

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

### 3.5.9. Automatische Relaisabschaltung nach Öffnung der Tür

Zutrittskontrolle:

Für die Zeit wie lange eine Tür geöffnet wird, gibt es in der Tabelle „Action“ eine Zeitangabe „Elapse“. Für die unter „Elapse“ angegebene Zeit wurde das Öffnen der Tür permanent auch angesteuert.

Nun kann die Zutrittskontrolle das Öffnungsrelais abschalten, sobald eine Tür-Öffnung erkannt wird. Voraussetzung ist, dass der Öffnungskontakt der Tür bauseits vorhanden und an das Zutrittskontrollsystem angeschlossen ist.

#### 3.5.9.1. Überwachte Türen

Eine überwachte Tür beschreibt ein Feature der Zutrittscontroller, welches es ermöglicht, Türen wieder zu verriegeln, nachdem diese geöffnet wurden. Jeder Tür wird dafür ein digitaler Eingang zugewiesen anhand dessen überprüft werden kann, ob diese geöffnet wurde. Überwachte Türen werden



Abbildung 1 Aufbau einer überwachten Tür

in der ReaderProps Liste konfiguriert. Wird nun eine Türöffnung festgestellt, so werden alle durch den Leser aktivierten Relais für die Türen wieder deaktiviert. Geprüft werden alle für ein Leser referenzierten Aktionen.



#### Hinweis:

Durch die Türüberwachung werden nur Relais abgeschaltet, die durch eine Buchung für begrenzte Zeit geöffnet wurden. Falls Türen durch eine Zeitsteuerung geöffnet, oder auf Dauer auf (Free Access) gestellt wurden, bleibt die Tür weiterhin geöffnet.



#### Achtung:

Es werden alle referenzierten Action Einträge auf Rücknahme geprüft. Auf eventuell referenzierte Gruppen wird nicht geachtet.

### 3.5.9.2. Konfiguration der überwachten Tür

Um überwachte Türen in der Zutrittskontrolle nutzen zu können, wird die ReaderProps Liste genutzt. Diese Liste wird auch für die EMA und für Antipassback genutzt. Die Angaben zu Größe der Spalten sind deshalb minimale Werte.

### 3.5.9.3. Aufbau des Eintrags in der ReaderProps Liste

Die ReaderProps Liste benötigt für überwachte Türen 5 Einträge.

Name	Type	Länge	Beschreibung
RefReader	Nummer	4	Referenz-Nummer des Lesers, dessen Relais-Schaltung zurückgenommen werden sollen
Type	Nummer	2	Typ der Erweiterung für den referenzierten Leser( 5 = Überwachtes Türmodul).
Mode	Nummer	1	Modus in der der Eingang gewertet wird 0 (Input Low) = die Tür ist geöffnet 1 (Input High) = die Tür ist geöffnet
RefReaderInput	Nummer	4	Referenz zu dem Leser (oder Türmodul oder Zutritts-Controller), an dem der Eingang zur Überwachung der Tür anliegt.
Input	Nummer	2	Nummer des Eingangs, welcher das Öffnen der Tür meldet. 0 = es findet keine Überwachung statt. 1-32 = Digitaler Eingang des Türkontakts

### 3.5.9.4. Prüfung der Türmodule in der Zutrittskontroller

Auf Controller-Seite werden im Rahmen der Zutrittskontrolle folgende Bedingungen geprüft:

Änderung eines digitalen Eingangs

Dient der Eingang zur Überwachung einer Tür?

Entspricht der Eingangswert dem eingestellten Modus?

Alle durch den Leser ausgelöste ZK-Aktion zurücknehmen

Fertig

(1) Beim Wechsel eines digitalen Eingangs wird die Prüfung der überwachten Tür gestartet.

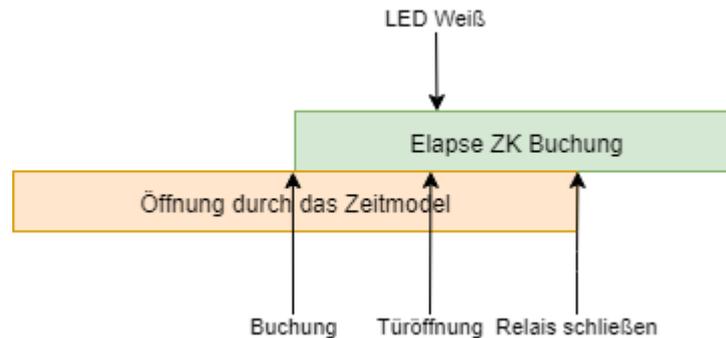
(2) Nun wird geprüft, ob der Eingang („Input“), sowie der zugehörige Leser („RefReaderInput“) in der Liste ReaderProps als Eingang für eine überwachte Tür eingetragen wurden.

(3) Ist dies der Fall, wird nun geprüft, ob der Wert des digitalen Eingangs dem Modus („Mode“) entspricht. Ist der digitale Eingang High (1) so muss der Modus auch 1 sein. Ist der digitale Eingang Low (0) so muss der Modus auch 0 sein. Ist der Modus korrekt wird nun der Zustand des Relais überprüft.

(4) Nun werden alle durch den referenzierte Leser („RefReader“) vorgenommen zeitlich begrenzten Öffnungen zurückgenommen. Falls das Relais auf Dauer Auf (FRA) oder Dauer Zu (BLA) steht, oder das Relais durch die Zeitsteuerung aktiviert wurde wird es nicht geöffnet.

### 3.5.9.5. Sonderfall zeitlich gesteuerte Relais

Während ein Zeitmodell aktiv ist, kann am Leser weiterhin gebucht werden. Die gewählte Elapseezeit der Buchung und die Zeit des Zeitmodells können sich dabei überschneiden.



Ein Konflikt tritt auf, falls die Tür vor dem Ablauf des Zeitmodells geöffnet wird. In diesem Fall wird die LED wieder weiß geschaltet. Das Relais wird dabei nicht angerührt. Das Relais wird dann mit Ende des Zeitmodells geschlossen.



#### Hinweis:

Beim Schalten des Relais durch ein Zeitmodell wird die LED nicht grün geschaltet. Auch bei Buchungen wird lediglich die LED für 3 Sekunden (Standard für erfolgreiche Buchung) geschaltet, und nicht entsprechend der hinterlegten Elapseezeit.

### 3.5.9.6. Beispiel Konfiguration

Als Beispiel wird der Aufbau aus Abbildung 1 genutzt. Der digitale Eingang 1 wird als Melder für eine geöffnete Tür genutzt. Ist der digitale Eingang auf Low, so ist die Tür geöffnet.

#### ZK-Listen

Zuerst werden die beiden Geräte in der Reader Liste als Leser definiert. Die ID 10 beschreibt den Leser, welcher die Tür öffnet. ID 99 beschreibt den Zutritts-Controller.

Reader.txt

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

In der Liste Action2 wird der Befehl zum Öffnen der Tür angegeben. Der Eintrag mit der ID 100 wird bei erfolgreicher Buchung auf dem Leser mit der ID 10 ausgeführt. Die Action schaltet das Relais 1 auf dem Controller für 10 Sekunden. Gleichzeitig wird die grüne LED auf dem Leser mit der ID 10 angeschaltet.

#### 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

In der Liste Time geben Sie ein Zeitmodell an. Das Zeitmodell 1 gilt jeden Tag und ist 24 Stunden aktiv.

#### Time.txt

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

In der Liste Location müssen wir einen Eintrag erstellen. Das Zeitmodell gibt an, dass eine Buchung am Leser immer möglich ist.

#### Location.txt

ID	RefGroup	RefTime	RefTimeNoPin
1	0	1	0

In der Liste Identification wird nun noch ein gültiger Ausweis definiert, um die Tür zu öffnen.

#### Identification.txt

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

### Zusätzliche Listen

Neben den ZK Listen wird die Setup Liste ReaderProps benötigt. Falls der Eingang 1 des Controllers auf low wechselt, so werden alle Türen, die durch eine ZK-Buchung zeitlich begrenzt entriegelt wurden, wieder verriegelt. Der Eintrag zur überwachten Tür aus Abbildung 1 sieht darin wie folgt aus:

#### ReaderPorps.txt

RefReader	Type	Mode	RefReaderInput	Input
10	5	0	99	1

### 3.5.10. Statusmeldungen der Zutrittskontrolle

Anzeige	ZK-mit Vorprüfung	Zugeordnete Statusmeldung
0		Modul erkannt, alles OK.
3		Modul in der Liste nicht definiert, aber im Bus gefunden.
4		Modul in der Liste, aber nicht im Bus gefunden.
5		Falsches Verschlüsselungspasswort.
6		Login-Passwort falsch.
7		Lesertyp (Mifare, Legic, Unique, etc.) falsch.
8		Fehler beim Konfigurieren des Moduls.
9		Modul weder im Bus noch in der Liste gefunden.
10		Der Kommunikationsschlüssel für das PHG-Crypt-Protokoll wurde geändert.
11		Der Kommunikationsschlüssel für das PHG-Crypt-Protokoll wurde nicht geändert.
12		Batteriezustand der Funkschließzylinder in Phase 0 (voll)
13		Batteriezustand der Funkschließzylinder in Phase 1
14		Batteriezustand der Funkschließzylinder in Phase 2
15		Batteriezustand der Funkschließzylinder in Phase 3 (leer)
16		Funkschließzylinder in Batteriewechselmodus gesetzt
17		Modul hat ein Update erhalten gilt für EVO Agera (ehem. EVO-Plus-Leser)
18		Modul hat ein Neustart nach Update durchgeführt
19	519	Zutritt verweigert, weil BLA (blocked Access) an diesem Leser aktiv ist
20	520	Ausweis korrekt, Zutritt gestattet.
21	521	Ausweis nicht in der Liste Identification.
22	522	ActiveGeneral passt nicht / gesperrter Ausweis
23	523	Gültigkeitszeitraum passt nicht. Zeitraum in der Identification abgelaufen oder noch nicht begonnen.
24	524	Keinen passenden Raum gefunden. In der Reader angegebene Raum fehlt in Location oder die Gruppe darf nicht in diesen Raum.
25	525	Keinen passenden Zeitbereich gefunden. Das in der Location angegebene Zeitmodell existiert nicht oder ist = „0“.
26	526	Warte auf eine Pin-Eingabe.
27	527	Pin falsch.
28	528	Bedrohungscode wurde eingegeben.
29	529	Die PIN ist korrekt, Zutritt gestattet.
30	530	Die Master-PIN wurde eingegeben, Zutritt gestattet.
31	531	PIN-Timeout wurde erreicht.
32	532	Master-Ausweis korrekt, Zutritt gestattet.
33	533	NUR-PIN-Eingabe ist korrekt, Zutritt gestattet.
34		Online-Transponder gelesen
35		Online-PIN.
36	536	Schließung durchgeführt
37	537	Freier Zutritt am Leser
38	538	Zutritt am Leser gesperrt / Leser blockiert /dauerhaft zu
39		Online-Ergebnis des Servers: Kein Zutritt gewährt
	256	Online-Ergebnis des Servers wurde ausgeführt.
	257	Online-Ergebnis des Servers wurde nicht ausgeführt.

Digitale	Ausgänge
40	Digitaler Ausgang 1 ist Low (Aus).
41	Digitaler Ausgang 1 auf HIGH.(An).
42	Digitaler Ausgang 1 für die Dauer ELAPSE auf HIGH.
43	Digitaler Ausgang 2 ist Low (Aus).
44	Digitaler Ausgang 2 auf HIGH.(An).
45	Digitaler Ausgang 2 für die Dauer ELAPSE auf HIGH.
46	Digitaler Ausgang 3 ist Low (Aus).
47	Digitaler Ausgang 3 auf HIGH.(An).
48	Digitaler Ausgang 3 für die Dauer ELAPSE auf HIGH.
49	Digitaler Ausgang 4 ist Low (Aus).
50	Digitaler Ausgang 4 auf HIGH.(An).
51	Digitaler Ausgang 4 für die Dauer ELAPSE auf HIGH.
52 #	Digitaler Ausgang 5 ist Low (Aus).
53 #	Digitaler Ausgang 5 auf HIGH.(An).
54 #	Digitaler Ausgang 5 für die Dauer ELAPSE auf HIGH.
55 #	Digitaler Ausgang 6 ist Low (Aus).
56 #	Digitaler Ausgang 6 auf HIGH.(An).
57 #	Digitaler Ausgang 6 für die Dauer ELAPSE auf HIGH.

## Statusmeldungen der Zutrittskontrolle

Anzeige	Zugeordnete Statusmeldung
Digitale	Ausgänge
120#	Digitaler Ausgang 7 ist Low (Aus).
121#	Digitaler Ausgang 7 auf HIGH.(An).
122#	Digitaler Ausgang 7 für die Dauer ELAPSE auf HIGH.
123#	Digitaler Ausgang 8 ist Low (Aus).
124#	Digitaler Ausgang 8 auf HIGH.(An).
125#	Digitaler Ausgang 8 für die Dauer ELAPSE auf HIGH.
126#	Digitaler Ausgang 9 ist Low (Aus).
127#	Digitaler Ausgang 9 auf HIGH.(An).
128#	Digitaler Ausgang 9 für die Dauer ELAPSE auf HIGH.
129#	Digitaler Ausgang 10 ist Low (Aus).
130#	Digitaler Ausgang 10 auf HIGH.(An).
131#	Digitaler Ausgang 10 für die Dauer ELAPSE auf HIGH.
132#	Digitaler Ausgang 11 ist Low (Aus).
133#	Digitaler Ausgang 11 auf HIGH.(An).
134#	Digitaler Ausgang 11 für die Dauer ELAPSE auf HIGH.
135#	Digitaler Ausgang 12 ist Low (Aus).
136#	Digitaler Ausgang 12 auf HIGH.(An).
137#	Digitaler Ausgang 12 für die Dauer ELAPSE auf HIGH.
138#	Digitaler Ausgang 13 ist Low (Aus).
139#	Digitaler Ausgang 13 auf HIGH.(An).
140#	Digitaler Ausgang 13 für die Dauer ELAPSE auf HIGH.
141#	Digitaler Ausgang 14 ist Low (Aus).
142#	Digitaler Ausgang 14 auf HIGH.(An).
143#	Digitaler Ausgang 14 für die Dauer ELAPSE auf HIGH.
144#	Digitaler Ausgang 15 ist Low (Aus).
145#	Digitaler Ausgang 15 auf HIGH.(An).
146#	Digitaler Ausgang 15 für die Dauer ELAPSE auf HIGH.
147#	Digitaler Ausgang 16 ist Low (Aus).
148#	Digitaler Ausgang 16 auf HIGH.(An).
149#	Digitaler Ausgang 16 für die Dauer ELAPSE auf HIGH.
300#	Digitaler Ausgang 17 ist Low (Aus).
301#	Digitaler Ausgang 17 auf HIGH.(An).
302#	Digitaler Ausgang 17 für die Dauer ELAPSE auf HIGH.
303#	Digitaler Ausgang 18 ist Low (Aus).
304#	Digitaler Ausgang 18 auf HIGH.(An).
305#	Digitaler Ausgang 18 für die Dauer ELAPSE auf HIGH.
306#	Digitaler Ausgang 19 ist Low (Aus).
307#	Digitaler Ausgang 19 auf HIGH.(An).
308#	Digitaler Ausgang 19 für die Dauer ELAPSE auf HIGH.
309#	Digitaler Ausgang 20 ist Low (Aus).
310#	Digitaler Ausgang 20 auf HIGH.(An).
311#	Digitaler Ausgang 20 für die Dauer ELAPSE auf HIGH.
312#	Digitaler Ausgang 21 ist Low (Aus).
313#	Digitaler Ausgang 21 auf HIGH.(An).
314#	Digitaler Ausgang 21 für die Dauer ELAPSE auf HIGH.
315#	Digitaler Ausgang 22 ist Low (Aus).
316#	Digitaler Ausgang 22 auf HIGH.(An).
317#	Digitaler Ausgang 22 für die Dauer ELAPSE auf HIGH.

Digitale	Eingänge
160#	Digitaler Eingang 7 auf Low
161#	Digitaler Eingang 7 auf High
162#	Digitaler Eingang 8 auf Low
163#	Digitaler Eingang 8 auf High
164#	Digitaler Eingang 9 auf Low
165#	Digitaler Eingang 9 auf High
166#	Digitaler Eingang 10 auf Low
167#	Digitaler Eingang 10 auf High
168#	Digitaler Eingang 11 auf Low
169#	Digitaler Eingang 11 auf High
170#	Digitaler Eingang 12 auf Low
171#	Digitaler Eingang 12 auf High
_____	_____fortlaufend bis:
210#	Digitaler Eingang 32 auf Low
211#	Digitaler Eingang 32 auf High

# neu für die EVO-Line V4 Geräte

EMA	Beschreibung
258 <sup>1</sup>	Nach einer EMA-Buchung an einem entsprechend konfigurierten PIN-Leser wird auf die Identifizierung (Transponder + ggf. Pin) gewartet.
259	Nach einer EMA-Buchung wurde nicht innerhalb von fünf Sekunden ein Ausweis vor den Leser gehalten, um die Buchung zu legitimieren.
260	Der vorgehaltene Ausweis zur Legitimation der EMA-Buchung ist nicht zugelassen. Entweder ist die Ausweisnummer unbekannt, der Ausweis ist in der Identification-Tabelle nicht für EMA-Schaltungen freigeschaltet oder die Gruppe hat keine EMA-Schaltberechtigung. (ActiveGeneral <b>nicht</b> auf 7)
261	Der eingegebene EMA-Bereich ist nicht richtig konfiguriert worden.
262	Während einer Scharf- oder Unscharfschaltung eines EMA-Bereiches ist für diesen Bereich keine weitere EMA-Aktion möglich.
263 <sup>1</sup>	Die EMA meldet per digitalem Eingang, dass sie zur Scharfschaltung bereit ist.
264 <sup>1</sup>	Die EMA meldet per digitalem Eingang, dass sie nicht zur Scharfschaltung bereit ist.
265	Per Steuersignal (Relais) wird einem EMA-Bereich mitgeteilt, dass er scharf schalten soll.
266	Per Steuersignal (Relais) wird einem EMA-Bereich mitgeteilt, dass er unscharf schalten soll.
267	Der scharf zu schaltende EMA-Bereich ist bereits scharf geschaltet. Am Leser wird dennoch „grün“ signalisiert, damit der Benutzer erkennt, dass die EMA scharf ist.
268	Der unscharf zu schaltende EMA-Bereich ist bereits unscharf geschaltet. Am Leser wird dennoch „grün“ signalisiert, damit der Benutzer erkennt, dass die EMA unscharf ist.
269 <sup>1</sup>	Der EMA-Bereich ist jetzt scharf.
270 <sup>1</sup>	Der EMA-Bereich ist jetzt unscharf.
271	Der EMA-Bereich konnte innerhalb von fünf Sekunden nicht scharf geschaltet werden. Der zugeordnete digitale Eingang meldet nach wie vor ‚unscharf‘.
272	Der EMA-Bereich konnte innerhalb von fünf Sekunden nicht unscharf geschaltet werden. Der zugeordnete digitale Eingang meldet nach wie vor ‚scharf‘.
273	Die Zutrittsbuchung wird wegen eines scharf geschalteten EMA-Bereiches abgewiesen.
274	Bei der Identifizierung wird zusätzlich eine PIN benötigt.
275	Die eingegebene PIN passt nicht zu der hinterlegten.
276	Die eingegebene PIN passt zu der hinterlegten.
277	Timeout bei der Pin-Eingabe

## Statusmeldungen der Zutrittskontrolle

Anzeige	Zugeordnete Statusmeldung																																																																			
100	Die ZK ist deaktiviert.																																																																			
101	Die ZK kann z.Zt. die Anfrage nicht bearbeiten.																																																																			
102	Die ZK benötigt die Listen.																																																																			
103	Der Bus-Typ (Datafox, PHG, ID-Tronic) passt nicht zu dem im Setup eingestellten Transponderverfahren, . Z.B.: Mifare+ HID, MyD, I-Code...etc.																																																																			
104	Fehler in der Anwesenheitssteuerung. Handle-Fehler in der Presence Liste																																																																			
105	Ereignis, dass das Inbetriebnahme-Menü für die ZK betreten wurde.																																																																			
106	Ereignis, dass das Inbetriebnahme-Menü für die ZK verlassen wurde.																																																																			
107	Ereignis, dass im Inbetriebnahme-Menü für die ZK bei den Relais Änderungen gemacht und beim Verlassen beibehalten wurden.																																																																			
108	Ereignis, dass der Inbetriebnahme-Modus für die ZK gestartet wurde.																																																																			
109	Ereignis, dass der Inbetriebnahmemodus für die ZK beendet wurde.																																																																			
110	Gemischter Betrieb PHG und Funkmodul (FSM) im gleichen Bus ist nicht zulässig.																																																																			
Anzeige	Zugeordnete Statusmeldung																																																																			
	<table border="1"> <thead> <tr> <th>Master (ZK-Box / ZK Master)</th> <th>GIS / TS-Serie</th> <th>PHG / EVO-ZK-Leser</th> </tr> </thead> <tbody> <tr> <td>60</td> <td>Digi. Eingang1 Master Low</td> <td>Digitaler Eingang1 Leser Low</td> <td>Digi.-1 (IO-Box geschlossen)</td> </tr> <tr> <td>61</td> <td>Digi. Eingang1 Master High</td> <td>Digitaler Eingang1 Leser High</td> <td>Digi.-1 (IO-Box offen)</td> </tr> <tr> <td>62</td> <td>Digi. Eingang2 Master Low</td> <td>Digitaler Eingang2 Leser Low</td> <td>Digi.-2 (IO-Box geschlossen)</td> </tr> <tr> <td>63</td> <td>Digi. Eingang2 Master High</td> <td>Digitaler Eingang2 Leser High</td> <td>Digi.-2 (IO-Box offen)</td> </tr> <tr> <td>64</td> <td>Digi. Eingang3 Master Low</td> <td>Digitaler Eingang3 Leser Low</td> <td>Digi. 3; Sabotageüberwachung -&gt; Kommunikationskanal OK</td> </tr> <tr> <td>65</td> <td>Digi. Eingang3 Master High</td> <td>Digitaler Eingang3 Leser High</td> <td>Digi. 3; Sabotageüberwachung -&gt; Kommunikation-unterbrochen</td> </tr> <tr> <td>66</td> <td>Digi. Eingang4 Master Low</td> <td>Digitaler Eingang 3 wurde unterbrochen</td> <td>PHG not used</td> </tr> <tr> <td>67</td> <td>Digi. Eingang4 Master High</td> <td>Digitaler Eingang 3 wurde kurz geschlossen</td> <td>PHG not used</td> </tr> <tr> <td>68</td> <td>Digi. Eingang5 Master Low</td> <td>not used</td> <td>not used</td> </tr> <tr> <td>69</td> <td>Digi. Eingang5 Master High</td> <td>not used</td> <td>not used</td> </tr> <tr> <td>70</td> <td>Digi. Eingang6 Master Low</td> <td>not used</td> <td>digi. Eingang 1 am Leser Low nicht bei der Voxio-E-Serie</td> </tr> <tr> <td>71</td> <td>Digi. Eingang6 Master High</td> <td>not used</td> <td>digi. Eingang 1 am Leser High nicht bei der Voxio-E-Serie</td> </tr> <tr> <td>72</td> <td></td> <td>not used</td> <td>digi. Eingang 2 am Leser Low nicht bei der Voxio-E-Serie</td> </tr> <tr> <td>73</td> <td></td> <td>not used</td> <td>digi. Eingang 2 am Leser High nicht bei der Voxio-E-Serie</td> </tr> <tr> <td>74</td> <td></td> <td>not used</td> <td>Sabotagekontakt → Gerätezustand OK</td> </tr> <tr> <td>75</td> <td></td> <td>not used</td> <td>Sabotagekontakt → Gerät manipuliert</td> </tr> </tbody> </table>	Master (ZK-Box / ZK Master)	GIS / TS-Serie	PHG / EVO-ZK-Leser	60	Digi. Eingang1 Master Low	Digitaler Eingang1 Leser Low	Digi.-1 (IO-Box geschlossen)	61	Digi. Eingang1 Master High	Digitaler Eingang1 Leser High	Digi.-1 (IO-Box offen)	62	Digi. Eingang2 Master Low	Digitaler Eingang2 Leser Low	Digi.-2 (IO-Box geschlossen)	63	Digi. Eingang2 Master High	Digitaler Eingang2 Leser High	Digi.-2 (IO-Box offen)	64	Digi. Eingang3 Master Low	Digitaler Eingang3 Leser Low	Digi. 3; Sabotageüberwachung -> Kommunikationskanal OK	65	Digi. Eingang3 Master High	Digitaler Eingang3 Leser High	Digi. 3; Sabotageüberwachung -> Kommunikation-unterbrochen	66	Digi. Eingang4 Master Low	Digitaler Eingang 3 wurde unterbrochen	PHG not used	67	Digi. Eingang4 Master High	Digitaler Eingang 3 wurde kurz geschlossen	PHG not used	68	Digi. Eingang5 Master Low	not used	not used	69	Digi. Eingang5 Master High	not used	not used	70	Digi. Eingang6 Master Low	not used	digi. Eingang 1 am Leser Low nicht bei der Voxio-E-Serie	71	Digi. Eingang6 Master High	not used	digi. Eingang 1 am Leser High nicht bei der Voxio-E-Serie	72		not used	digi. Eingang 2 am Leser Low nicht bei der Voxio-E-Serie	73		not used	digi. Eingang 2 am Leser High nicht bei der Voxio-E-Serie	74		not used	Sabotagekontakt → Gerätezustand OK	75		not used	Sabotagekontakt → Gerät manipuliert
Master (ZK-Box / ZK Master)	GIS / TS-Serie	PHG / EVO-ZK-Leser																																																																		
60	Digi. Eingang1 Master Low	Digitaler Eingang1 Leser Low	Digi.-1 (IO-Box geschlossen)																																																																	
61	Digi. Eingang1 Master High	Digitaler Eingang1 Leser High	Digi.-1 (IO-Box offen)																																																																	
62	Digi. Eingang2 Master Low	Digitaler Eingang2 Leser Low	Digi.-2 (IO-Box geschlossen)																																																																	
63	Digi. Eingang2 Master High	Digitaler Eingang2 Leser High	Digi.-2 (IO-Box offen)																																																																	
64	Digi. Eingang3 Master Low	Digitaler Eingang3 Leser Low	Digi. 3; Sabotageüberwachung -> Kommunikationskanal OK																																																																	
65	Digi. Eingang3 Master High	Digitaler Eingang3 Leser High	Digi. 3; Sabotageüberwachung -> Kommunikation-unterbrochen																																																																	
66	Digi. Eingang4 Master Low	Digitaler Eingang 3 wurde unterbrochen	PHG not used																																																																	
67	Digi. Eingang4 Master High	Digitaler Eingang 3 wurde kurz geschlossen	PHG not used																																																																	
68	Digi. Eingang5 Master Low	not used	not used																																																																	
69	Digi. Eingang5 Master High	not used	not used																																																																	
70	Digi. Eingang6 Master Low	not used	digi. Eingang 1 am Leser Low nicht bei der Voxio-E-Serie																																																																	
71	Digi. Eingang6 Master High	not used	digi. Eingang 1 am Leser High nicht bei der Voxio-E-Serie																																																																	
72		not used	digi. Eingang 2 am Leser Low nicht bei der Voxio-E-Serie																																																																	
73		not used	digi. Eingang 2 am Leser High nicht bei der Voxio-E-Serie																																																																	
74		not used	Sabotagekontakt → Gerätezustand OK																																																																	
75		not used	Sabotagekontakt → Gerät manipuliert																																																																	
Anzeige	Zugeordnete Statusmeldung																																																																			
80	Alarm Eingang 1																																																																			
81	Alarm Eingang 2																																																																			
82	Alarm Eingang 3																																																																			
83	Alarm Eingang 4																																																																			
84	Alarm Eingang 5																																																																			
85	Alarm Eingang 6																																																																			
220#	Alarm Eingang 7																																																																			
221#	Alarm Eingang 8																																																																			
_____	_____ fortlaufend bis:																																																																			
245#	Alarm Eingang 32																																																																			
250	Anti-passback hard (ein doppelter Zutritt in einem Raum ist nicht möglich)																																																																			
251	Anti-passback soft, für eine angegebene Zeit unter Duration																																																																			

# neu für die EVO-Line V4 Geräte

## Statusmeldungen einbinden:

### Hinweis:

Um die Statusmeldungen zu erhalten, muss mit der Funktion im Setup „Zutritt Status übernehmen“, der Statuswert in den Datensatz geschrieben werden.



Feldbezeichnung, entsprechend Datensatzbeschreibung:

Feldfunktion:

### 3.5.11. Statusanzeige der Zutrittsmodule über LEDs

Gelb	Grün	Rot	Zustand des TS TMR33-xx
aus	aus	aus	Es liegt keine Versorgungsspannung an
an	aus	aus	Es liegt eine Versorgungsspannung an, Leser vom Master erkannt und konfiguriert Zustand nach Modultest = Status „OK“
an	an (ca. 1 s)	an (ca. 1 s)	Akustisches Signal durch Summer (ca. 1s) signalisiert Modultest
an	aus	an (ca. 10 s)	Die Listen des Zutrittsmasters werden aktualisiert
an	aus	an (Dauer)	Konfigurationsfehler über die Zutrittslisten (Prüfung der Statusmeldungen notwendig.)
blinkt	aus	aus	Signalisiert lesbare Karte im Bereich, oder der Leser ist von Master nicht erkannt
an	an (ca. 1 s)	aus	Gelesene Karte ist Zutrittsberechtigt, zusätzlich akustisches Signal durch Summer (ca. 1s)
an	an	an 3 x kurz	Gelesene Karte ist nicht Zutrittsberechtigt
an	blinkt	aus	Es wird eine PIN Eingabe erwartet

### 3.5.12. Onlinefunktionen der Zutrittskontrolle

Sie haben die Möglichkeit, bei der Steuerung der Zutrittskontrolle (ZK) alle Entscheidungen und Aktionen der ZK in Ihre Software zu legen.

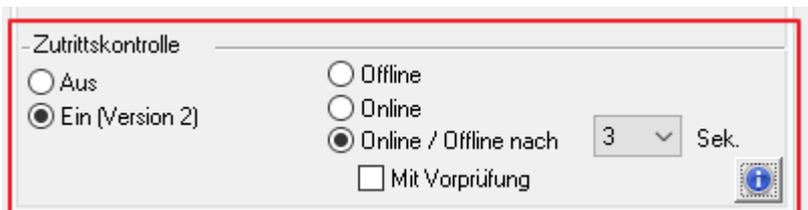
Somit können Sie in Echtzeit auf alle Anforderungen an einer ZK reagieren.

Im Setup unter „Grundeinstellung“ wird die Onlinefunktion der ZK aktiviert.



Es gibt hier 2 Möglichkeiten:

- nur **Online** Modus (es wird immer auf eine Antwort / Reaktion vom Server gewartet)
- im **Online/Offline** wird eine eingestellte Zeit auf eine Antwort gewartet. Ist die Zeit verstrichen, werden die internen ZK-Listen zur Prüfung verwendet.



#### 3.5.12.1. Online über HTTP-Anbindung

Die Übertragung der Daten an einen Webserver ist eine sehr schnelle und einfach einzubindende Kommunikationsmöglichkeit. Dies ermöglicht es, über die Antwort des Webserver sehr schnell auf Ereignisse aus der ZK zu reagieren. Damit ist eine echte „Online Funktionalität“ der Zutrittskontrolle mit Datafox- Geräten gegeben.

Voraussetzung

Hardware:

- TCP/IP
- GPRS (1-2 Sekunden Verzögerung)

Software:

- aktives Skript mit Logik für die ZK und abgestimmt auf die angeschlossene Hardware (ZK-Leser)

Über die Rückantwort können Sie entsprechende Aktionen auf den Zutrittslesern durchführen: Die nachfolgenden Beispiele geben Ihnen einen Einblick über die Funktionen / Aktionen. Alle zu übergebenden Parameter entsprechen der Onlinefunktion über die DLL.

## Beispiel 1:

Folgende Daten wurden z.B. empfangen.

`table=Zutritt&Datum_Uhrzeit=2013-07-05_07%3A48%3A11&Master_ID=1&Modul_ID=010&Ausweis_Nr=2058&Status=34&checksum=2461`

Master_ID=1	Master-ID
Modul_ID=010	Busadresse des Lesers / TM
Ausweis_Nr=2058	Ausweisnummer
Status=34	Online (34)

### Passende Antwort, um Zutritt zu gewähren:

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

*ab der Firmware 04.03.04 ebenfalls möglich ist:*

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

<b>access=010</b>	Busadresse, auf der die Aktion durchgeführt werden soll bis FW 04.03.03
<b>module=010</b>	Busadresse auf dem geschaltet werden soll
<b>master=1</b>	Bus-Strang auf dem geschaltet werden soll
<b>mask=8</b>	Relais Nr.1
<b>type=1</b>	einschalten
<b>duration=1</b>	für 1 Sekunde

### Passende Antwort, um Zutritt zu verweigern, rote LED Ein:

`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`

<b>access=010</b>	Busadresse, auf der die Aktion durchgeführt werden soll
<b>module=010</b>	Busadresse, auf der die Aktion durchgeführt werden soll
<b>master=1</b>	Bus-Strang auf dem geschaltet werden soll
<b>mask=5</b>	Rote LED + Buzzer
<b>type=1</b>	einschalten
<b>duration=2</b>	für 2 Sekunden

Mit der neuen Hardware V4 können mehrere Bus-Stränge angesteuert werden. Um auf dem entsprechenden Bus-Strang Aktionen ausführen zu können, muss die Bus-Strang ID mit der Antwort mit übergeben werden.

Hierzu wurden die neuen Schlüsselwörter „**module**“ und „**master**“ eingeführt. Diese müssen zusammen genutzt werden und ersetzen somit das Schlüsselwort „**access**“.



#### Achtung:

Die Reihenfolge „**access**□**mask**→**typ**→**duration**“ oder **master**→**module**→**mask**→**typ**→**duration** muss unbedingt eingehalten werden.

`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`

## Übersicht über die möglichen Parameter für die Schlüsselwörter:

Schlüsselwort	Wert / Bit Nr.	Beschreibung
<b>access=</b> oder <b>module=</b> Funktion für 1x Bus RS485	000 010 011 ... 081 usw.	Der Wert der Zeichenfolge, muss dem Format des Feldes "TM" der "Reader" Liste folgen. Er muss demnach immer 3 Ziffern umfassen.
<b>master =</b>	1-3 1 2	Id für den RS485 Bus ZK, Beschreibt den ZK-Bus-Strang. RS485 Bus ID 1 RS485 Bus ID 2 usw. „ <b>master</b> “ muss gemeinsam mit „ <b>module</b> “ eingesetzt werden und ersetzt damit „ <b>access</b> “
<b>mask</b>	1 / 0 2 / 1 4 / 2 8 / 3 16 / 4 32 / 5 64 / 6 128 / 7 256 / 8 ....	Bei gesetztem Bit, wird der Buzzer angesprochen. Bei gesetztem Bit, wird die grüne LED angesprochen. Bei gesetztem Bit, wird die rote LED angesprochen. Bei gesetztem Bit, wird das <b>1 Relais</b> angesprochen. Bei gesetztem Bit, wird das <b>2 Relais</b> angesprochen. Bei gesetztem Bit, wird das <b>3 Relais</b> angesprochen. Bei gesetztem Bit, wird das <b>4 Relais</b> angesprochen. Bei gesetztem Bit, wird das <b>5 Relais</b> angesprochen. Bei gesetztem Bit, wird das <b>6 Relais</b> angesprochen. Unbenutzt. Bitte immer auf 0 setzen.
<b>type</b>	0 1 2 3	Aus Ein Wechsel (600ms an, 600ms aus) 3 mal einschalten für 500ms
<b>duration</b>	Sekunden / 0	Ist eine Zeitdauer und nur bei type = 1 gültig. Bedeutung: 0 = ständig ein, 1 - 40 = Sekunden ein.



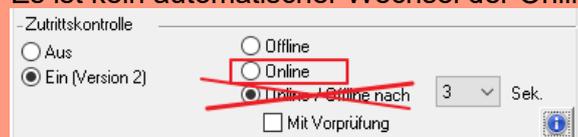
### Hinweis:

Sie können auch mehrere Aktionen für die ZK in einer Antwort ausführen. Die Gesamtlänge der Antwort darf dabei allerdings nicht **254 Zeichen überschreiten**.



### Achtung:

Es ist kein automatischer Wechsel der Online /Offline ZK über HTTP möglich,



Es ist nur der Online-Modus möglich.

### 3.5.12.2. Online über DLL-Anbindung

Die DLL bietet Funktionen, um die externen Leser der ZK direkt anzusteuern. Mit der Funktion „DFCEntrance2OnlineAction“ können der Buzzer, die LEDs oder die Relais auf einem Zutrittsmodul per DLL geschaltet werden.

Bei einer Zutrittsbuchung erzeugt der Zutrittsmaster einen Datensatz. Dieser muss sofort abgeholt und zur Anwendung auf dem Server weitergeleitet werden. Die Anwendung entscheidet dann, ob Zutritt gewährt wird und gibt einen Befehl zur Ansteuerung des Relais im Türmodul zurück oder lässt den Buzzer ertönen und gibt über die LED's eine optische Meldung aus.

Mehr Informationen über die Funktionalitäten der DLL finden Sie in der Schnittstellenbeschreibung. [https://www.datafox.de/downloads-software-masteriv-hardwareversion-v4.de.html?file=files/Datafox\\_Devices/Downloads\\_Geraete\\_Zubehoer/001\\_MasterIV-Software/Datafox\\_SDK\\_Windows\\_04.03.11.zip](https://www.datafox.de/downloads-software-masteriv-hardwareversion-v4.de.html?file=files/Datafox_Devices/Downloads_Geraete_Zubehoer/001_MasterIV-Software/Datafox_SDK_Windows_04.03.11.zip)

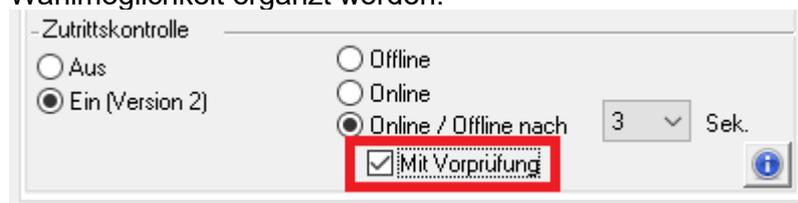
### 3.5.13. Online/Offline-Zutrittskontrolle mit Vorprüfung

Die Funktion „Online/Offline-Zutrittskontrolle mit Vorprüfung“ (OOZKmV) erweitert die Zutrittskontrolle um die Berechnung eines Zutrittsvorschlags, der dann online geprüft und akzeptiert bzw. verworfen werden kann. Der Server muss nur die Entscheidung treffen, ob die Person berechtigt ist, einen Raum zu betreten oder nicht. Die Ansteuerung der Relais und die Rückmeldung an den Leser erfolgt eigenständig durch den Zutrittscontroller.

#### 3.5.13.1. Konfiguration der Online/Offline-Zutrittskontrolle mit Vorprüfung

##### 3.5.13.2. Einstellungen im Setup

In den Grundeinstellungen des Setups ist im Konfigurationsbereich der Zutrittskontrolle eine weitere Wahlmöglichkeit ergänzt worden:



Diese setzt voraus, dass das Gerät, auf dem die OOZKmV eingesetzt wird, eine vollständige Parametrierung der Zutrittskontrolle hat.

##### 3.5.13.3. Betriebsmodus der Zutrittskontrolle ermitteln

Der Modus, in dem die Zutrittskontrolle läuft, kann über die Systemvariable „access.mode“ ermittelt werden. Hier werden folgende Status-Codierungen verwendet:

access.mode	Beschreibung
0	Offline-ZK
1	Online-ZK
2	Online/Offline-ZK
3	Online/Offline-ZK mit Vorprüfung

##### 3.5.13.4. Ablauf der Online/Offline-Zutrittskontrolle mit Vorprüfung

Im Betriebsmodus OOZKmV wird für ein Zutrittsereignis zunächst die Zutrittsprüfung durchgeführt, wie diese in den Offline-Betriebsmodi ebenfalls durchgeführt werden würde. Diese führt nicht zum Schalten eines Relais sondern wird als Vorprüfungsdaten (Status-Code + 500) als Datensatz für den Server bereitgestellt.

Der Server nimmt den Datensatz entgegen und quittiert diesen per DLL oder über HTTP.

- Erfolgt dieses innerhalb des Online/Offline-Timeouts (oben auf 3 Sekunden eingestellt), so wird die Entscheidung, die der Server übermittelt, umgesetzt und ein Datensatz mit Status-Code 256 oder 257 erzeugt.
- Läuft das Offline-Timeout ohne Antwort des Servers ab, so generiert die ZK einen weiteren Datensatz mit dem normalen Zutritts-Statuscode (also der Wert, der im Vorprüfungsdatensatz eingetragen war - 500).

Online /offline

Pre-checkedMode	Discription/ Beschreibung
256	Zutritt bei Online mit Vorprüfung: Der Server lehnt die Vorprüfung ab
257	Zutritt bei Online mit Vorprüfung: Der Server stimmt der Vorprüfung zu

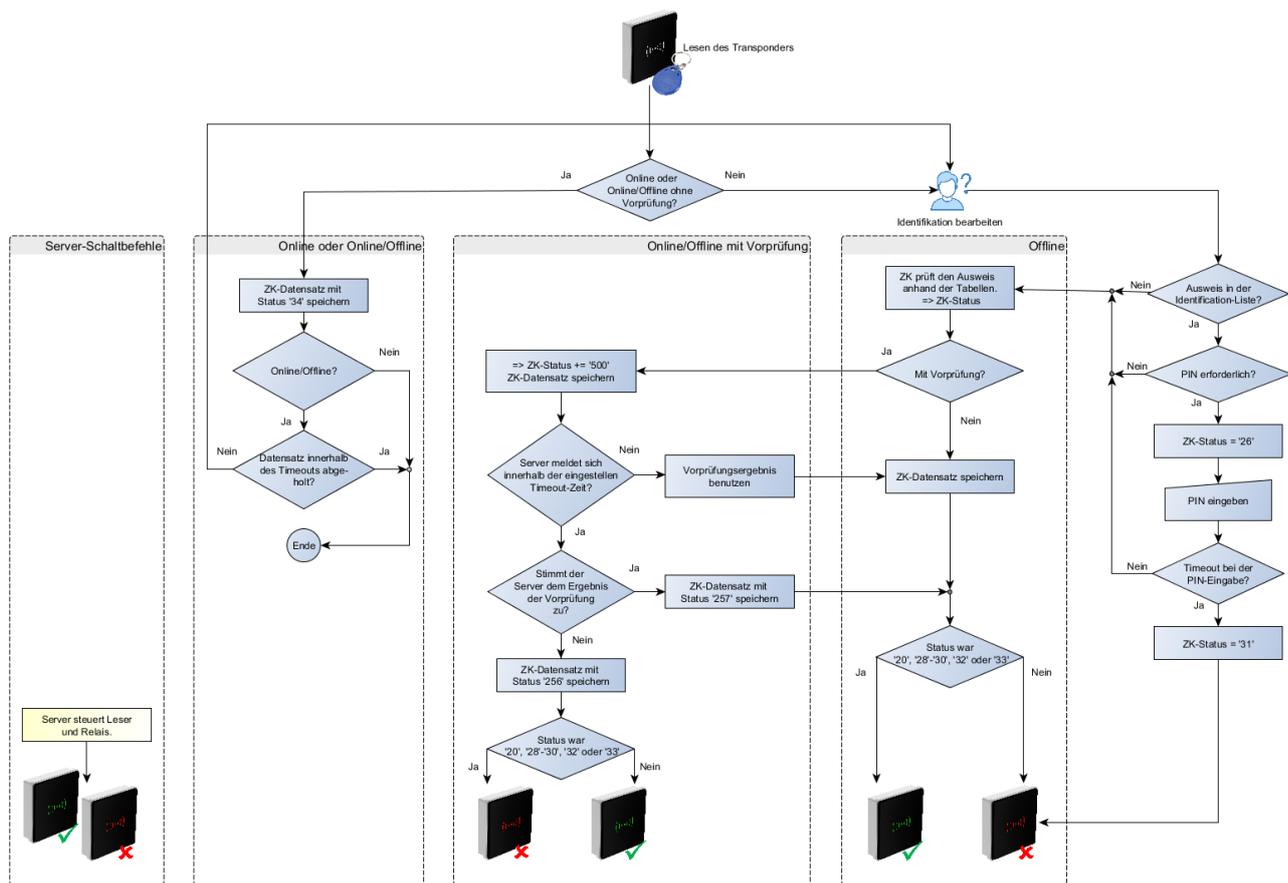


Abbildung: Auswertung der Zutrittsprüfung

Die Darstellung des grünen Lesers im Diagramm bedeutet gleichzeitig, dass das Tür-Relais geöffnet wird.

### 3.5.13.5. Quittierung des Vorprüfungsdatensatzes

### 3.5.13.6. HTTP-Schnittstellen: Methode df\_ao\_ac2

Mit der HTTP Schnittstelle steht eine eigene Methode zum Quittieren eines Vorprüfungsdatensatzes zur Verfügung. Zusätzlich zum „df\_api=1“ wird hier der Parameter df\_ao\_ac2 (ao = Assisted Online, ac2 = Access Control 2) mit folgendem Aufbau erwartet:

Parametername	Bedeutung
Mode	Entscheidung des Servers. <ul style="list-style-type: none"> <li>• 0 = Aktion ablehnen</li> <li>• 1 = Aktion annehmen</li> </ul>
Group	ID der Gruppe. Falls in der Action2-Liste eine Gruppen-ID zur Öffnung benötigt wird. (Die Ausweis-ID befindet sich nicht in der Identification-Liste)

Beispiele:

```
df_ao_ac2=1
df_ao_ac2=0,1234
```

### 3.5.13.7. DLL-Funktion: DFCQuitRecordExt()

Über die DLL wird eine Datensatz der OZKmV mittels DFCQuitRecordExt() quittiert. Der Parameter-String param wird dabei identisch zum HTTP-Response erwartet, d.h. hier wird auch ein „df\_ao\_ac2=1“ (oder Ähnliches) erwartet.

Auszug aus der DLL-Dokumentation:

#### DFCQuitRecordExt()

```
DF_API_EXTERN int DF_API_CALL DFCQuitRecordExt ( int    connectionId,  
                                                int    deviceAddress,  
                                                char * param,  
                                                int *  paramLength  
                                                )
```

Datensatz im Gerät quittieren.

Es wird versucht einen zuvor mit [DFCReadRecord\(\)](#) gelesenen Datensatz zu quittieren. Nach erfolgreicher Quittierung kann mit einem folgenden Aufruf von DFCReadRecord der ggf. nächste Datensatz gelesen werden.

#### Export

DFComDLL als DFCQuitRecordExt  
DFCom\_x64 als DFCQuitRecordExt

#### Parameter

- [in] **connectionId** Zu verwendende Verbindungs-ID.
- [in] **deviceAddress** Anzusprechende Geräteadresse.
- [in,out] **param** Zeichenfolge als Parameterstring. Wird 1:1 an die Firmware weitergegeben.
- [in,out] **paramLength** Als *in* die Länge des auf *param* verweisenden Puffers, als *out* die nach *param* kopierte Länge des Antwortparameters.

#### Rückgabewerte

- 1 Fehler bei Ausführung.
- 0 Keine Quittung benötigt.
- 1 Online-Datensatz quittiert.
- 2 Wiederholt einen Online-Datensatz quittiert.
- 3 Offline-Datensatz quittiert.
- 4 Wiederholt einen Offline-Datensatz quittiert.

#### Seit

04.03.12 enthalten.

### **3.5.13.8. Sonderfall: Identifikation nicht möglich**

Liegt bei einem Zutrittsereignis kein Eintrag zum Transponder in der Identification-Tabelle vor, so bedeutet das „Ablehnen“ dieses Zutritt-Verweigert-Ereignisses durch den Server, dass der Zutritt gewährt werden soll.

Um hier eine Aktion im Zutritts-Datenmodell auslösen zu können, ist es erforderlich, die Gruppe zu kennen, deren Ereignis ausgelöst werden soll, da zu dieser unbekanntem ID ja keine Aktion hinterlegt ist.

Diese Gruppe muss dann zusätzlich beim Quittieren des Vorprüfungsdatensatzes übermittelt werden.

Mit diesem Mechanismus können z.B. Besucherausweise ohne Übertragung von Listen auf den Zutrittscontroller direkt im Server abgebildet werden.

### 3.5.14. Funktionen für ZK und U&Z

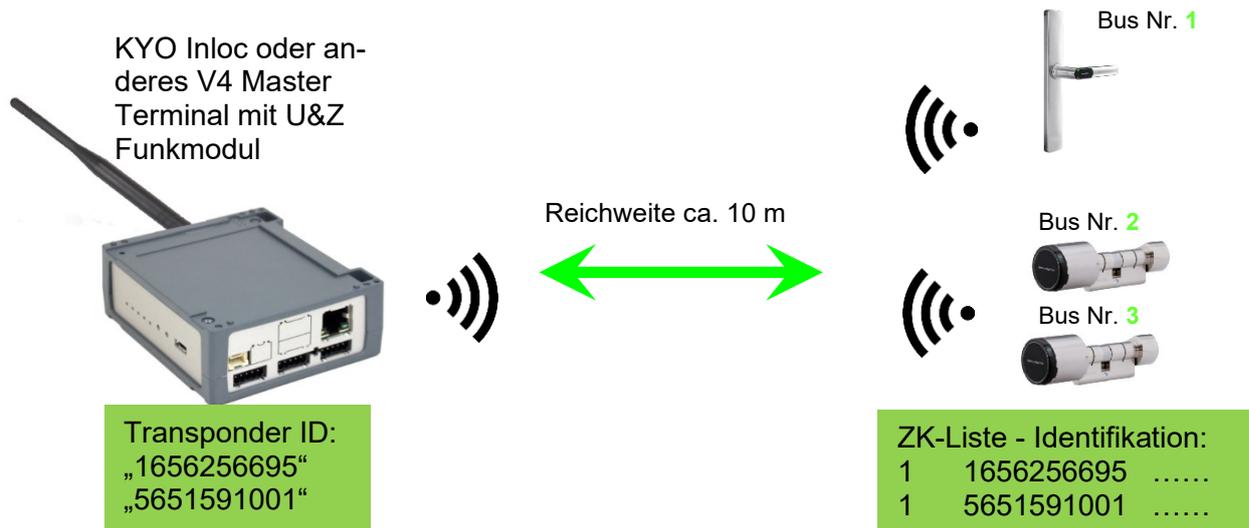
#### 3.5.14.1. Aufbaubeispiel

Der Aufbau bzw. das Einbinden der Funkschließzylinder erfolgt über die Standard Datafox Zutrittskontrolle. Dabei kommt das PHG-Crypt-Protokoll zum Einsatz. Somit sind alle Daten sicher Verschlüsselt.

Funktionsweise:

Die elektronischen Schließsysteme lesen einen RFID-Chip / Karte und übermitteln die gelesenen Informationen an die Datafox ZK. Die Datafox ZK entscheidet dann anhand der Zutrittslogik ob die Tür geöffnet wird oder nicht.

#### Aufbaubeispiel mit integriertem Funkmodul in dem KYO-Inloc.



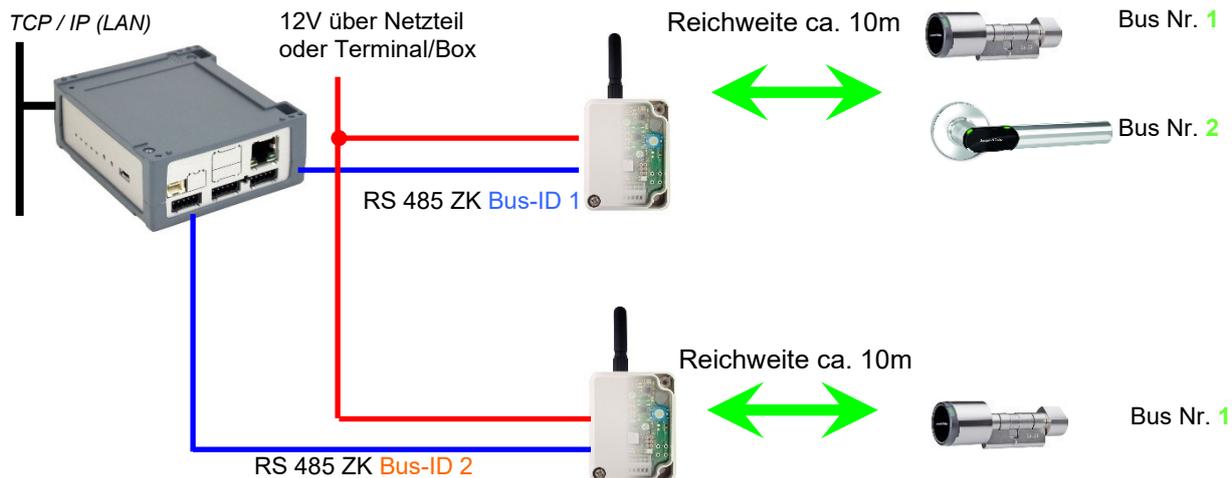
Entsprechende Reader Tabelle, Beispiel:

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

**Hinweis:**  
 Die Transponder werden vom Zylinder gelesen und die ID an die ZK-Box übertragen. Diese entscheidet dann, ob die ID Zutritt erhält und sendet ein entsprechendes Signal an den Zylinder.

**Hinweis:**  
 Es kann immer nur mit einem Funkschließzylinder gearbeitet werden!  
 Von der Buchung bis zur Beendigung der Funkverbindung benötigen wir ca. 2 Sekunden bei einer Abweisung. Bei einer Öffnung ca. 1 Sekunde.  
 Werden an zwei oder mehreren Türen exakt zur gleichen Zeit Ausweise vorgehalten, hat der erste Schließzylinder die Verbindung mit dem FSM für ca. 2 Sekunden. Wenn nach 1 Sekunde ein Funkschließzylinder keine Funkverbindung erhält, macht er eine Offlineprüfung. Sind keine Ausweise hinterlegt, reagiert er auf den Ausweis nicht mehr. Der Ausweis wird dann im Leser gespeichert und es wird nicht mehr auf diesen Ausweis reagiert (Buchungswiederhol Sperre) bis ein anderer Ausweis vorgehalten wurde.

## Aufbaubeispiel KYO Cenloc V4 mit zwei externen Funkmodulen.

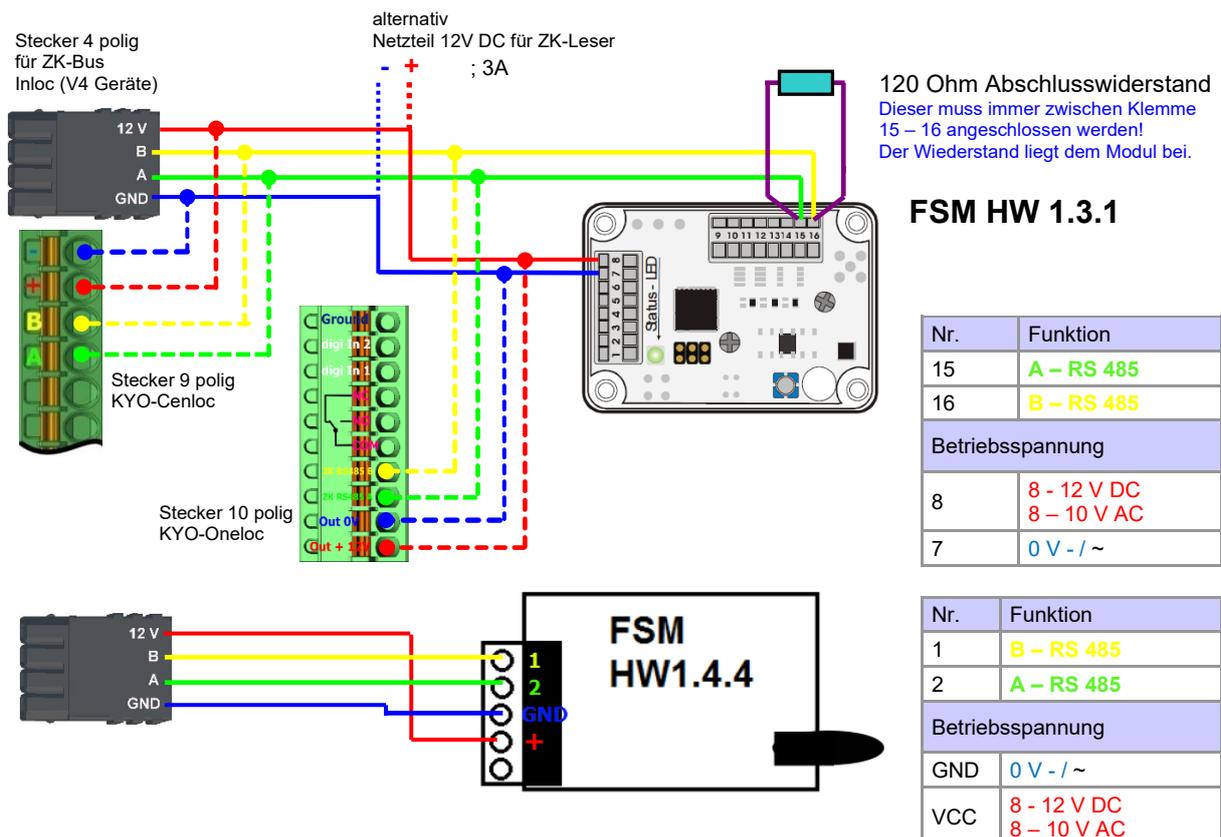


Entsprechende Reader Tabelle, Beispiel:

ID	ZM / Bus-ID	TM (Busadresse)	RefLocation	RefAction	PinGeneral	Description text
1	1	010	1	1	0	Leser an RS485 Modulplatz 1 = Bus ID 1
2	1	020	2	2	0	Leser an RS485 Modulplatz 3 = Bus ID 1
3	2	010	3	3	0	Leser an RS485 Modulplatz 7 = Bus ID 2
4	1	320	0	1	0	KYO Inloc (Mastergerät)

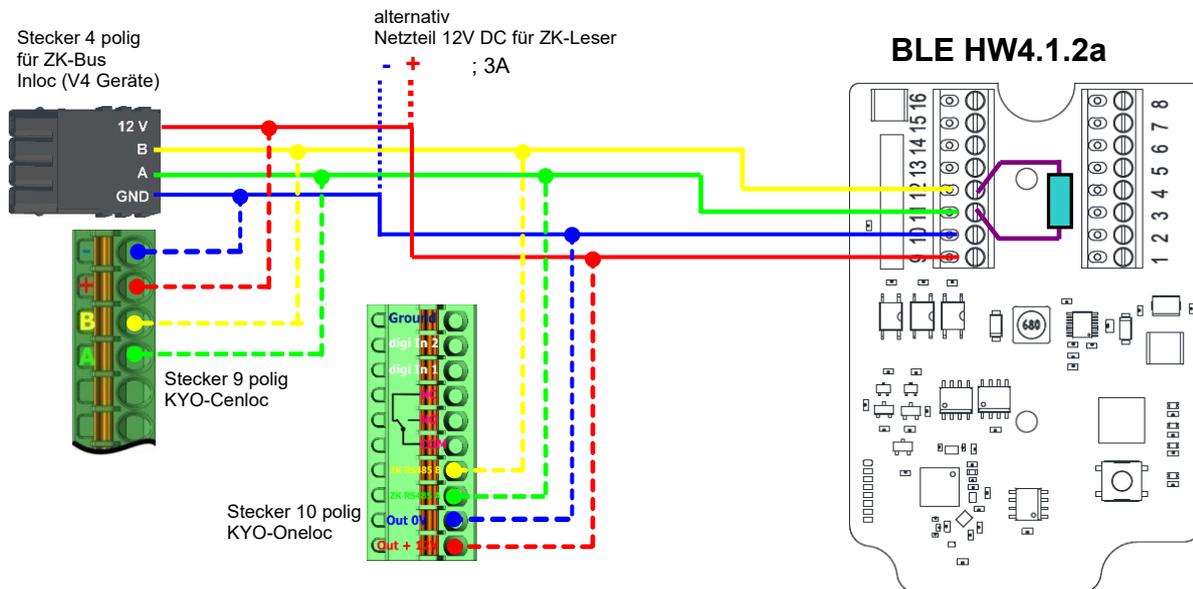
## Verdrahtungsplan der verschiedenen ZK-Busanschlüsse mit externem Funkmodul 868 MHz:

(hierbei gilt der gleiche Aufbau pro ZK-Strang bzw. ZM / Bus-ID)



**Verdrahtungsplan der verschiedenen ZK-Busanschlüsse mit externem BLE-Modul:**  
 (hierbei gilt der gleiche Aufbau pro ZK-Strang bzw. ZM / Bus-ID)

120 Ohm Abschlusswiderstand  
 Dieser muss immer zwischen Klemme  
 11 – 12 angeschlossen werden!  
 Der Widerstand liegt dem Modul bei.



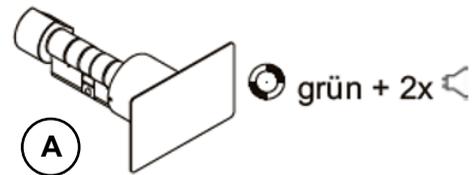
Nr.	Funktion
11	RS 485 - A
12	RS 485 - B
Betriebsspannung	
GND	0 V
VCC	5 - 24 V DC

### 3.5.14.2. Inbetriebnahme der Schließzylinder

Zum Lieferumfang gehört immer eine Service-Karte.  
Für den Einbau der Zylinder benötigen Sie auch eine Demontage-Karte  
und zum Wechseln der Batterien die Batteriewechsel-Karte.  
Im Auslieferungszustand sind diese noch nicht angelegt.

#### **Servicekey vor das Knaufmodul halten. (A)**

- Ein optisches/akustisches Signal zeigt an, dass der Programmiermodus aktiv ist  
(evtl. ist vor diesem Schritt das Wecken des Knaufmoduls durch Andrehen erforderlich)



Mit der Firmware 2.7.0 erfolgt nur eine akustische Signalisierung über Aktivierung des Servicemodus!

#### **Anlernen:**

- 1.) die erste Karte die vorgehalten wird = Batteriewechselkarte
- 2.) die zweite Karte wird zur = Demontagekarte

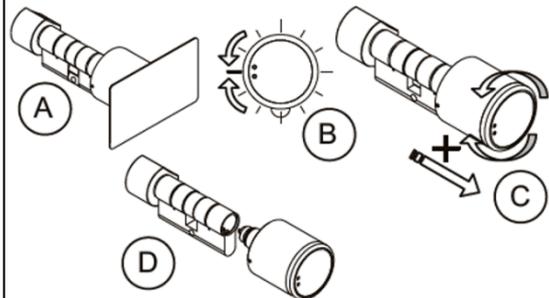
### 3.5.14.3. Montage und Demontage der Zylinder

1.) Demontagekarte vor das Knaufmodul halten (A)  
(evtl. ist vor diesem Schritt das Wecken des Knaufmoduls durch Andrehen erforderlich).

2.) Knaufmodul fährt in den Demontagemodus.

3.) Das Knaufmodul solange drehen, bis sich die Notstromkontakte auf ca. 9 Uhr-Position befinden. (B)

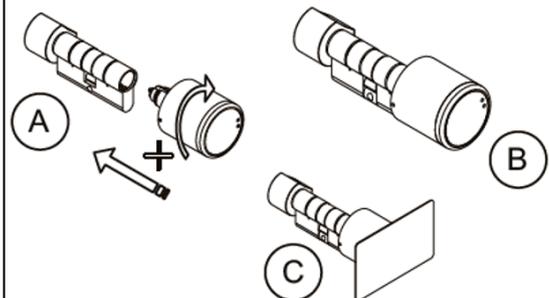
4.) Den Knauf durch geringfügiges Hin- und Herdrehen und gleichzeitiges leichtes Ziehen demontieren. (C+D)



1.) Führen Sie die Schritte 1 und 2, wie im Punkt oben beschrieben durch (nicht erforderlich, wenn sich das Knaufmodul noch im Demontagemodus befindet).

2.) Das Knaufmodul wird durch Einstecken und gleichzeitiges Drehen in das Zylindergehäuse montiert. (A+B)

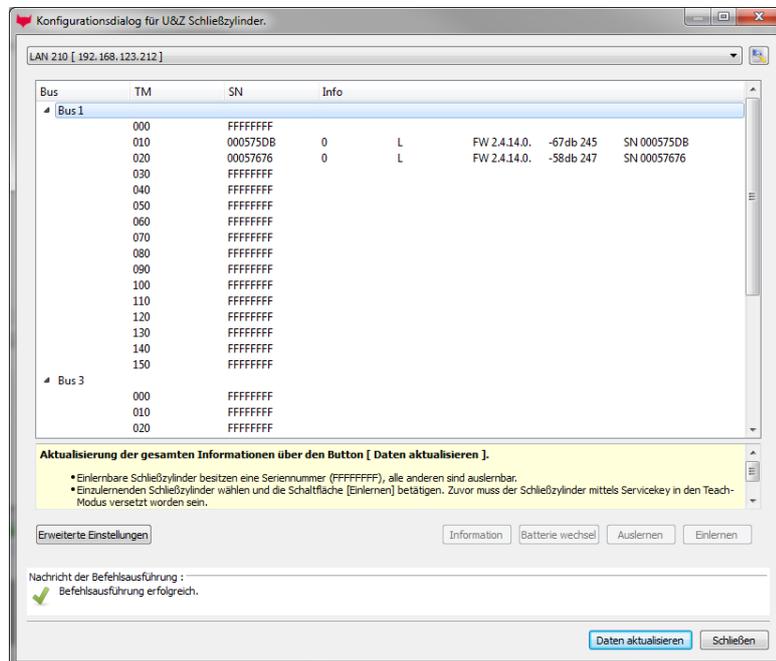
3.) Um den Demontagemodus zurückzusetzen, die Demontagekarte oder einen berechtigten Transponder vor das Knaufmodul halten. (C)



### 3.5.14.4. Einrichten des Funknetzwerkes

Zum Einrichten kann das DatafoxStudioIV in Verwendung mit der Service-Key-Karte verwendet werden. Dazu im DatafoxStudioIV unter "Konfiguration→Zutrittskontrolle→Schließzylinder U&Z konfigurieren" auswählen. Mit "Daten aktualisieren" wird die aktuelle Konfiguration aus den FSM gelesen.

In Verbindung mit dem BLE-Modul können nur die Adressen 000 – 070 angelernt werden.



## Schritte des Einlernens der Zylinder:

### 1. Service-Key an Zylinder vorhalten

(Service = 20 Sekunden aktiv (Zylinder aktivieren durch kurzes Drehen!))

### 2. Daten aktualisieren betätigen im DatafoxStudioIV!

Freie Adressen werden mit FFFFFFFF dargestellt, bei den vergebenen Adressen steht die Seriennummer des Funkschließzylinders und der Status der Module wie beim Dialog Status der Zutrittsmodule. Zum Einlernen eines neuen Funkschließzylinders eine freie Adresse markieren und anschließend auf Einlernen klicken (Innerhalb der Service-Zeit).

Über den Dialog "Konfigurationsdialog für U&Z Schließzylinder" sind verschiedene Dinge möglich.

- Erweiterte Einstellungen
  - Festlegen der ZK-Master ID für das Gerät
  - KnobActiveTime: Zeit, die der Zylinder nach Aktivierung versucht das FSM zu erreichen, bis er wieder in den Standby geht
- Informationen zum einzelnen Schließzylinder (Spalte „Info“) aktualisieren
- Batteriewechsel versetzt den Funkschließzylinder in einen Modus, dass die Haube abgenommen und die Batterie gewechselt werden kann. Dazu muss kurz mit dem FSM kommuniziert werden. Dies wird durch Drehen des Knaufs oder vorhalten eines Transponders erreicht.
- Auslernen: Der Zylinder wird vom FSM entfernt und kann an einen anderen FSM eingelernt werden.
- Einlernen: Um einen Funkschließzylinder mit dem FSM zu verbinden (der Funkschließzylinder kommuniziert dann nur noch mit diesem FSM)



#### **Achtung:**

Vergewissern Sie sich der Schließzylinder nicht an zwei Funkmodulen gleichzeitig angelernt werden.

### 3.5.14.5. Batteriewechsel / Status / Lebensdauer



Bei „Open“ wird der Befehl zum Öffnen an das FSM gesendet. Dieser hält den Befehl solange vor bis eine Funkverbindung zustande kommt. Das kann durch Drehen oder Vorhalten eines Transponders realisiert werden. Anschließend werden die Sperrbolzen der Haube entriegelt.

Bei „Close“ wird der Befehl zum Verriegeln der Haubenbolzen wieder an das FSM gesendet. Die Verriegelung wird aber erst nach einer Gutbuchung / Öffnung hergestellt.

## Die drei Phasen des Batteriemanagements

### Phase 1

Wird ein berechtigter Ausweis vor das Knaufmodul gehalten, wird die Schließberechtigung gemäß Programmierung erteilt. Die Türöffnung wird aber mit 5x rotem Blinken (LED) und gleichzeitigen 5 kurzen akustischen Signalen begleitet.

### Phase 2

Wird ein berechtigter Ausweis vor das Knaufmodul gehalten, wird die Schließberechtigung gemäß Programmierung erst nach ca. 5 Sekunden erteilt. Während dieser 5 Sekunden blinkt die LED grün. Die Türöffnung wird mit 5x rotem Blinken (LED) und gleichzeitigen 5 kurzen akustischen Signalen begleitet.

### Phase 3

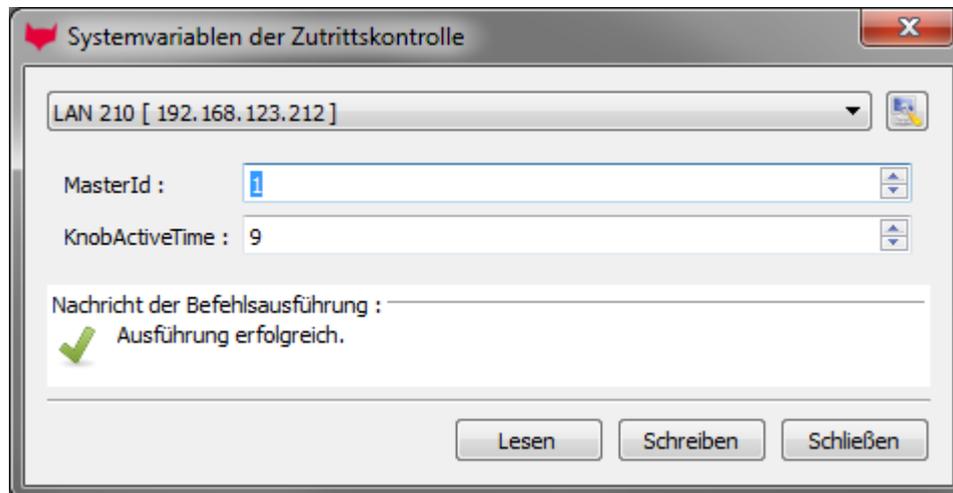
Das Knaufmodul reagiert nicht mehr auf berechnigte Ausweise. Ein Batteriewechsel ist unverzüglich vorzunehmen. Dieser ist nun nur noch mithilfe der Batteriewechselkarte möglich.

Beachten Sie bitte auch die entsprechenden Statusmeldungen aus der ZK:

Anzeige	Zugeordnete Statusmeldung
0	Modul erkannt, alles OK.
12	Batteriezustand der Funkschließzylinder in Phase 0 (voll)
13	Batteriezustand der Funkschließzylinder in Phase 1
14	Batteriezustand der Funkschließzylinder in Phase 2
15	Batteriezustand der Funkschließzylinder in Phase 3 (leer)
16	Funkschließzylinder in Batteriewechselmodus gesetzt

### 3.5.14.6. Wechseln der ZK-Master ID / Knob Active Time

Zum Wechseln der ZK-Master ID muss über den Dialog "Konfigurationsdialog für U&Z Schließzylinder" eingegeben werden. Darin befindet sich "Erweiterte Einstellungen" und mit einem Klick darauf öffnet sich dieser Dialog.



Master ID ist im Bereich von 1 bis 9999 setzbar. Besitzt ein Gerät mehr als einen ZK Bus, so ist die ZK-Master ID die ID des ersten Busses. Der zweite Bus ZK-Master ID + 1 usw.

Die Knob Active Time ist zum Voreinstellen, wie lange ein Funkschließzylinder die Funkkommunikation zum FSM aufrechterhält, wenn er aktiviert wurde. Bei einer Transponderbuchung schließt der ZK-Master automatisch die Verbindung nach Absetzen der Signalisierung und Öffnung. Ist die Knob Active Time kleiner als für die Transponderbuchung benötigt, schaltet der Funkschließzylinder ab und eine Öffnung schlägt fehl. Das passiert bei z.B. Knob Active Time = 1 (1s). Dreht jemand am Knauf des Funkschließzylinders, wird die Funkverbindung zum FSM aufgebaut und die Verbindung bleibt solange aktiv wie die Knob Active Time ist. Sinnvolle Werte sind zwischen 2 bis 10 Sekunden. Standardmäßig ist diese Zeit auf 3 Sekunden eingestellt.

Eine Erhöhung des Wertes ist sinnvoll, wenn an ein Funkmodul drei oder mehr Funkteilnehmer angebunden sind. Empfehlung: KnobActiveTime = 6 Sekunden

### 3.5.14.7. Optische und akustische Signale des U&Z Schließzylinders

Funktion	Töne	Optische Signale
Ruhemodus		
Beginn Programmiermodus	– ○	🟢 (außer bei FW 2.7.0)
Ausweis angelernt	○ ○	🟢
Ausweis gelöscht	– –	🔴
Warnsignal Alle Ausweise löschen	○ ○ ○ ○ ○ 15 sek.	🟢
Ende Programmiermodus	○ –	
Nach Wecken - Lesemodus		🔴
Ausweis nicht berechtigt	– – –	🔴
Ausweis berechtigt	○	🟢
Nach Batteriewechsel	– – –	🟢 🔴
Keine Funkverbindung (außer Reichweite)	Kein Ton	🔴 lang 🔴 kurz 🔴 kurz

🔴 = rot leuchtet

🔴 = rot blinkt

🟢 = grün leuchtet

🟢 = grün blinkt

– = langer tiefer Ton

○ = kurzer hoher Ton

### 3.5.14.8. Optische und akustische Signale des U&Z Türdrückers

Funktion	Töne	Optische Signale
Ruhemodus		
Beginn Programmiermodus	- O	
Ende Programmiermodus	O -	
Ausweis angelernt	O O	●
Ausweis gelöscht	- -	●
Nach Wecken - Lesemodus		●
Ausweis nicht berechtigt	- - -	●
Ausweis berechtigt	O	●
Reset	-	● ●
Batteriewarnung Phase1	O O O O O	● ● ● ● ●
Batteriewarnung Phase2	O O O O O	● ● ● ● ● ●

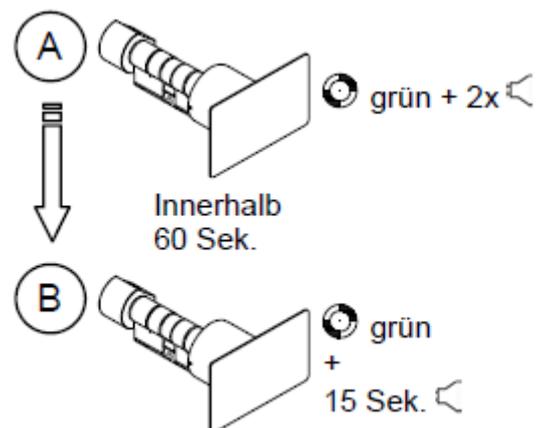
● = rot leuchtet      ● = rot blinkt  
 ● = grün leuchtet      ● = grün blinkt

- = langer tiefer Ton

O = kurzer hoher Ton

### 3.5.14.9. Zurücksetzen des U&Z Schließzylinders

- 1.) Das Knaufmodul muss in dem Funkmodul angelernt sein.
- 2.) Servicekey über die Dauer eines Programmiermodus (15 Sek.) vor das Knaufmodul halten und den Vorgang innerhalb 60 Sekunden wiederholen. Dies löscht am Ende des zweiten Programmiermodus alle Ausweise (inkl. Batteriewechsel- und Demontagekarte) bis auf den Servicekey. (A+B)
- 3.) Im Anschluss können die vorhandenen Ausweise, wie in Punkt 9.1 beschrieben, wieder angelernt werden.  
**Hierbei wird der erste vorgehaltene Ausweis zur Batteriewechselkarte und der zweite zur Demontagekarte.**



### 3.5.14.10. Hinweise zum Service Key

#### Service Key:

Für Service- und Programmiervorgänge an Schließsystemen der Baureihe Clex private ist als Nachweis der Berechtigung ein **Service Key** erforderlich. Der Service Key wird nach Auslieferung am Schließsystem eingelernt. Im Onlinebetrieb (Funk) kann nur dieser eine Service Key für Service verwendet werden. Ein Service Key sollte pro Unternehmensstandort einmalig vorhanden sein.



#### Anwendungsfälle

- Anlernen von Batteriewechsel-Karte und Demontage-Karte.
- Einlernen und löschen von Offline Berechtigungen, wenn Funk nicht verfügbar.
- Alle Ausweise löschen
- Anlernen an das Funkmodul.

#### System Card:

Für den Fall, dass der Servicekey beschädigt wird oder verloren geht, kann mit der Systemcard ein Ersatz-Servicekey bestellt werden. Daher ist die Systemcard sicher und für unbefugte unzugänglich aufzubewahren.

**Folgende Möglichkeiten bestehen, um einen Service Key zu ersetzen!**

**Alle Vorgänge können nur mit ausgeschaltetem Funk durchgeführt werden!**



#### Servicekey durch Servicekey ersetzen

Ein Servicekey kann durch einen anderen ersetzt werden. Aktuellen Servicekey vor das Knaufmodul halten, bis Programmiermodus aktiv ist. Neuen Servicekey vor Leseinheit halten, bis ein optisches/akustisches Signal zeigt, dass dieser angelesen ist.

#### Servicekey durch Ersatz Servicekey ersetzen

Für den Fall, dass der Servicekey beschädigt wird oder verloren geht, kann mit der Systemcard ein Ersatz-Servicekey bestellt werden. Der Ersatz-Servicekey ersetzt den verlorenen Servicekey.

#### Servicekey durch Klon Servicekey erweitern

Für den Fall, dass ein weiterer Servicekey innerhalb einer SystemCard benötigt wird, kann mit der Systemcard ein Servicekey Klon bestellt werden. Der Klon Servicekey ist kein 1:1 Duplikate ! Der Klon eignet sich für zusätzliche Standorte unterhalb einer SystemCard.

Wird der Klon an ein neues Schließsystem (Auslieferungszustand) eingelernt, dann ist der wie ein Standard Service Key auch im Funk-Betrieb verwendbar.

Ist der Klon nicht der erste eingelernte Servicekey dann greift seine Service-Funktion nur im Offline-fall (Ohne Funk). Im Online-Fall wird er ignoriert.

### 3.5.14.11. Unterstützte Transponderverfahren und Einschränkungen

#### **Transponder für 125kHz**

unterstützt wird

- Lesen Unique
- Lesen Hitag1
- Lesen Hitag2 **nur Seriennummer**

**nicht unterstützt wird**

- Lesen von Hitag2 Segmenten
- Lesen von Titan, Q5 und ATA5577

#### **Mifare Classic**

unterstützt wird

- Lesen UID
- Lesen Sektor/Block

**nicht unterstützt wird**

- Autologin (für Lesen alle Passwörter)

#### **Mifare Plus**

unterstützt wird nur Security Level 1

- Lesen UID
- Lesen Sektor/Block

**nicht unterstützt wird**

- Autologin (Für Lesen auch die Standardpasswörter verwenden)
- Random UID (Echte UID bei Random UID Ausweisen lesen)

#### **Mifare Desfire**

unterstützt wird

- Lesen UID
- Lesen Datei (max. 220Byte)

**nicht unterstützt wird**

- Random UID (Echte UID bei Random UID Ausweisen lesen)

#### **Legic Prime und Legic Advant**

aktuell sind keine Einschränkungen bekannt.

### 3.5.14.12. Servicekey beschädigt / verloren

Für den Fall, dass ein Autorisierungsmedium beschädigt wird oder verloren geht, kann mit der Systemcard ein Ersatz-Servicekey (CX2352) bei U&Z bestellt werden. Daher ist die Systemcard sicher und für unbefugte unzugänglich aufzubewahren.

### 3.5.14.13. Servicekey ersetzen

Ein Servicekey kann durch einen anderen ersetzt werden.  
Vorgehensweise:

1. Aktuellen Servicekey vor das Knaufmodul halten, bis Programmiermodus aktiv ist.
2. Neuen Servicekey vor das Knaufmodul halten, bis ein optisches/akustisches Signal zeigt, dass dieser angelernt ist.

### 3.5.14.14. Technische Daten des Funkmoduls

Technische Daten CX 6932	
<p><b>Abmessungen</b> Funkschaltmodul ohne Antenne: 65x50x40 mm Funkschaltmodul mit Antenne: 111x50x40 mm</p>	<p><b>Umweltbedingungen</b> Betriebstemperatur: -20°C bis 65°C Lagertemperatur: -40°C bis 85°C Einbauort: Innen- und Außenbereich (je nach Produktausführung). Abschattungen vermeiden! Beim Einsatz im Außenbereich sind die äußeren Rahmenbedingungen zu prüfen.</p>
<p><b>Stromversorgung</b> Versorgungsspannung: 8-20V= oder 8-16 V~ Stromverbrauch: Typ. 10mA (Ruhe), max. 50mA (Senden/Empf.)</p>	

### 3.5.15. Dauer-Öffnung bei Uhlmann&Zacher Funkbeschlägen

Dieses Kapitel beschreibt den Ablauf einer Dauer-Öffnung mittels eines Funk-Schließzylinders oder eines Funk-Türbeschlags (beides zusammen: U&Z-Beschlag) von Uhlmann und Zacher (U&Z).

### 3.5.16. U&Z-Dauer-Öffnung einer Tür (Variante 1 – Sicherer Betriebsmodus)

In der Parametrierung wird einem Ausweis eine Öffnungsdauer zugeordnet. Diese Öffnungsdauer kann entweder explizit über die Elapse-Zeit der Action2 oder implizit über ein zugeordnetes Zeitmodell vorgegeben werden. Ist die resultierende Öffnungsdauer länger als 3 Sekunden (typisch für normale Öffnungen sind 3 Sekunden), so ist der Ausweis „dauer-öffnungsberechtigt“<sup>1</sup>.

#### 3.5.16.1. Aktivieren der Daueröffnung

Wird ein Ausweis vor einen U&Z-Beschlag gehalten, so baut dieser die Verbindung zum Zutrittskontrollsystem auf. Stellt das ZK-System fest, dass

- keine Dauer-Öffnungsberechtigung für den Ausweis vorliegt, wird eine normale Zutrittsbuchung ausgewertet. Die Signalisierung erfolgt normal, d.h. grün für Zutritt gewährt, rot für Zutritt verweigert.
- eine Dauer-Öffnungsberechtigung vorliegt, so wird das Funk-Modul als „Dauer-Auf“ bis zum Ablauf des zugeordneten Zeitbereichs markiert, und der Zutritt gewährt.

#### 3.5.16.2. Bedienung während Dauer-Öffnung

Im Betriebszustand „Dauer-Auf“ kann die Tür ohne oder „normal“ mit einem Ausweis geöffnet werden – die Signalisierung erfolgt dann bei ungültigem Ausweis durch rot, bei gültigem Ausweis durch rot und grün<sup>2</sup>. Damit kann ein berechtigter Ausweis zur Kontrolle des „Dauer-Auf“ eingesetzt werden. In allen Fällen kann die Tür geöffnet werden – sie befindet sich im Betriebszustand „Dauer-Auf“.

Nach einer Öffnungsberechtigung – egal ob Dauer-Auf oder normaler Zutritt – koppelt das Tür-System nach etwa 5 Sekunden autark aus (in eingekuppeltem Zustand kann die Tür geöffnet werden, in ausgekuppeltem Zustand ist dieses nicht möglich).

Wird nun ein Tür-System betätigt, so baut dieses eine Funk-Verbindung zum Zutrittskontrollsystem auf. Ist hier für das Tür-System der Zustand „Dauer-Auf“

- aktiv, so gibt das Zutrittskontrollsystem den Auftrag zum Einkuppeln des Tür-Systems, so dass die Tür geöffnet werden kann.
- nicht aktiv, so wird eine normale Zutrittsbuchung erwartet.

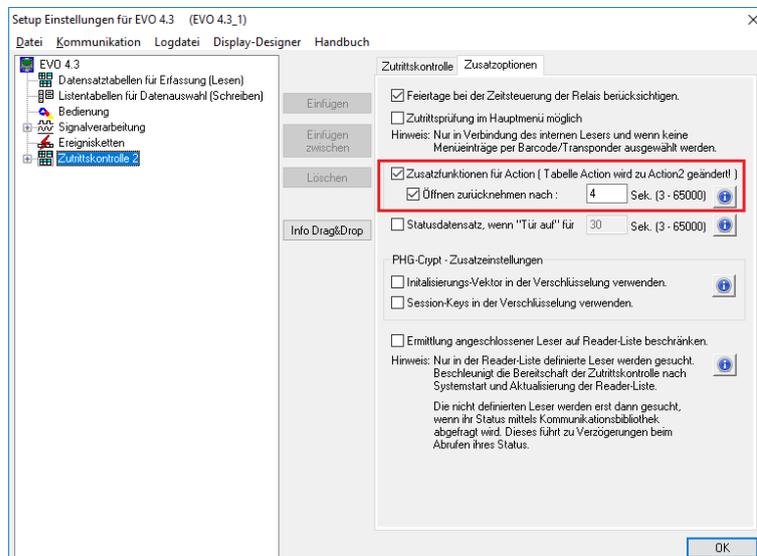
Hinweis: Bitte berücksichtigen Sie, dass das Aufbauen der Funkverbindung und damit das Prüfen, ob eine Tür aktuell im Betriebszustand „Dauer-Auf“ ist, eine bis zwei Sekunden in Anspruch nehmen kann. In dieser Zeit führt das Betätigen des Funk-Beschlags nicht zu einer Öffnung der Tür – die Tür kann erst nach dem Überprüfen des „Dauer-Auf“-Zustandes geöffnet werden. Diese Überprüfung wird durch das Aufblinker der grünen LED signalisiert.

<sup>1</sup> Falls Sie einen Zeitbereich und eine Elapse-Zeit einstellen, gilt die Logik, dass innerhalb des Zeitbereichs für die Elapse-Zeit geöffnet wird. Ist der Zeitbereich also von 08:30 bis 16:00 mit einer Elapse-Zeit von einer Stunde eingestellt, so kann um 15:59 eine Dauer-Öffnung bis 16:59 durchgeführt werden. Diese wird dann nicht um 16:00 zurückgenommen.

<sup>2</sup> Die uns bekannten Türbeschläge haben nur eine mehrfarbige LED zur Signalisierung. Daher mischen sich hier rot und grün zu gelbem Licht.

### 3.5.16.3. Rücknahme einer Dauer-Öffnung

Soll eine Dauer-Öffnung vor Ablauf des eingestellten Zeitbereichs zurückgenommen werden, muss dies über das Setup unter den Zusatzoptionen der Zutrittskontrolle eingestellt werden. Unter der Option „Öffnen zurücknehmen nach:“ kann der Zeitbereich in Sekunden eingestellt werden. Durch zweimaliges Vorhalten eines öffnungsberechtigten Ausweises innerhalb dieses Zeitbereiches (4 Sekunden im Screenshot) wird die Dauer-Öffnung zurückgenommen.



Das erste Vorhalten des Ausweises wird durch die rote und grüne LED gleichzeitig signalisiert, gefolgt von einem Beep des Funk-Beschlags. Nach dem Beep läuft das Zeitfenster für das zweite Vorhalten des Ausweises. Erfolgt dieses in der erwarteten Zeit, so wird das Rücknehmen der Dauer-Öffnung durch die grüne LED signalisiert, gefolgt von einem kurzen Beep.

### 3.5.16.4. Zusammenfassung

Dieses Verfahren ermöglicht eine Dauer-Öffnung von Türen mit U&Z-Beschlägen, die

- hinsichtlich der Energiebilanz optimal ist (es wird keine dauerhafte Funk-Verbindung benötigt)
- bei Strom-Ausfall in den verriegelten Zustand übergeht.

### 3.5.17. U&Z-Dauer-Öffnung einer Tür (Variante 2 – Klassischer Modus)

Im klassischen Modus koppelt das Schloss des Funk-Beschlags dauerhaft ein, so dass der Beschlag während der Dauer-Öffnungsperiode als normaler Tür-Knauf bzw. Tür-Klinke funktioniert.

#### 3.5.17.1. Daueröffnung mithilfe des klassischen Modus

Bei der Variante des klassischen Modus wird einem Ausweis eine spezielle Berechtigung gegeben, um den Modus (de-)aktivieren zu können. Nach der Aktivierung ist der Zylinder dauerhaft eingekuppelt und die Tür kann sofort geöffnet werden. Eine Freigabe durch das Steuergerät ist nicht notwendig.

Nach dem Deaktivieren kuppelt der Zylinder wieder aus. Danach ist die Tür wieder verschlossen und steht auch für normale Zutrittsbuchungen wieder zur Verfügung.

Zum Aktivieren des klassischen Modus muss mit dem Ausweis, der die spezielle Berechtigung besitzt, zweimal innerhalb von 15 Sekunden (nachfolgend Buchungswiederholungszeitraum) an dem Zylinder gebucht werden. Dasselbe gilt für das Deaktivieren des klassischen Modus.

Der Ausweis muss zwischen den beiden Buchungen aus dem Lesebereich des Zylinders genommen werden. Der Buchungswiederholungszeitraum ist fest vorgegeben und kann nicht eingestellt werden.

#### **Achtung:**



Diese Variante der Daueröffnung ist im Vergleich zu der Variante mit der hohen Schaltzeit für das Relais sehr unsicher, da bei Stromausfall, dem Ausfall des Steuergerätes oder Funkverbindungsproblemen zwischen dem Zylinder und dessen Funkmodul die Tür weiterhin ständig offen bleibt. Daher wird als Variante für die Daueröffnung mit der hohen Schaltzeit für das Relais empfohlen.

#### 3.5.17.2. Einrichten der Daueröffnung mithilfe des klassischen Modus

Um den klassischen Modus bei einem Zylinder aktivieren zu können, muss in der „Identification“-Liste für einen Ausweis bei „ActiveGeneral“ eine „6“ eingetragen werden. Der Eintrag muss zusätzlich zur „normalen“ Zutrittsnutzung (ActiveGeneral = 1) hinterlegt werden. Der Ausweis ist damit aktiviert und kann den klassischen Modus bei den Zylindern (de-)aktivieren. Dieser Ausweistyp wird nachfolgend mit Dauer-Auf-Ausweis bezeichnet.

Beispiel für einen solchen Eintrag in der „Identification“-Liste:

Id	Group	Pin	Duress	ActiveStart	ActiveEnd	ActiveGeneral
123456	1	0	0	2022-01-01	2023-01-01	1
<b>123456</b>	<b>1</b>	<b>0</b>	<b>0</b>	<b>2022-01-01</b>	<b>2023-01-01</b>	<b>6</b>

### 3.5.17.3. LED- und Buzzer-Signalisierungen des Zylinders im klassischen Modus

Nachfolgend werden die Signalisierungen des Tür-Beschlags erläutert.

Nr.	Zustand vor Aktion	Aktion	Zustand nach Aktion	Grüne LED	Rote LED	Relais
1	Klassischer Modus <b>nicht aktiv</b>	Normale gültige Zutrittsbuchung oder erste Buchung eines Dauer-Auf-Ausweises	Klassischer Modus <b>nicht aktiv</b>	2x kurz blinken + 1x piepen	-	Wird für X Sekunden geschaltet
2		Ungültige Zutrittsbuchung		-	3x kurz blinken + 3x piepen	Wird nicht geschaltet
3		Zweite Buchung desselben Dauer-Auf-Ausweises <b>außerhalb</b> des Buchungswiederholungszeitraums		Siehe 1	Siehe 1	
4		Zweite Buchung durch einen anderen Dauer-Auf-Ausweis <b>innerhalb</b> des Buchungswiederholungszeitraums				
5	Klassischer Modus <b>aktiv</b>	Zweite Buchung desselben Dauer-Auf-Ausweises <b>innerhalb</b> des Buchungswiederholungszeitraums	Klassischer Modus <b>aktiv</b>	2x kurz blinken + 2x piepen	-	Wird dauerhaft geschaltet
6		Gültige, ungültige oder erste Zutrittsbuchung eines Dauer-Auf-Ausweises		1x kurz blinken + 1x piepen		
7		Zweite Buchung eines Dauer-Auf-Ausweises <b>außerhalb</b> des Buchungswiederholungszeitraums				
8		Zweite Buchung durch einen anderen Dauer-Auf-Ausweis <b>innerhalb</b> des Buchungswiederholungszeitraums				
9		Zweite Buchung desselben Dauer-Auf-Ausweises <b>innerhalb</b> des Buchungswiederholungszeitraums	Klassischer Modus <b>nicht aktiv</b>	-	2x kurz blinken + 2x piepen	Wird dauerhaft ausgeschaltet

### **3.5.18. Bedienung /Aktivierung-Deaktivierung des Office-Mode**

#### **3.5.18.1. Aktivierung**

1 Vorhalten des Office-Mode berechtigten Ausweises

Klinke blinkt grün

2 Klinke betätigen und / oder mindestens 3 Sekunden warten bis die erste (normale) Öffnung an der Klinke durchgeführt wurde und Ausweis aus dem Feld (von der Klinke weg) nehmen. (Hinweis: während des Schaltvorgangs der Klinke werden keinen Buchungen von der Klinke angenommen).

3 Innerhalb der 15 Sekunden erneut Ausweis vorhalten.

Klinke blinkt grün, grün mit 2 kurzen Piep-Tönen.

Der Office-Mode ist somit aktiv!

#### **3.5.18.2. Deaktivierung**

1 Vorhalten des Office-Mode berechtigten Ausweises

Klinke blinkt grün

2 Karte muss aus dem Feld genommen (von der Klinke weg) werden.

3 Innerhalb der 15 Sekunden erneut Ausweis vorhalten.

Klinke blinkt rot, rot mit 2 kurzen Piep-Tönen.

Der Office-Mode ist somit deaktiviert!

### 3.5.18.3. Hinweise

- An einem Zylinder kann immer nur eine Variante der Daueröffnung durchgeführt werden: Entweder die Daueröffnung mithilfe einer hohen Schaltzeit für das Relais oder die Daueröffnung mithilfe des klassischen Modus.
- Wenn bei einem Ausweis „ActiveGeneral“ auf „6“ eingestellt ist (Dauer-Auf-Ausweis), dann kann auch eine Schaltzeit für das Relais größer als drei Sekunden eingestellt werden. Diese sollte allerdings höchstens zehn Sekunden betragen und nicht über das Zeitmodell geschehen, damit die zweite Buchung innerhalb von 15 Sekunden erfolgen kann.
- Wenn ein Ausweis für den klassischen Modus vorgesehen ist (unabhängig ob dieser zum Zeitpunkt der Buchung aktiv ist oder nicht), dann ist die Daueröffnung mithilfe einer hohen Schaltzeit für das Relais nicht möglich.
- Das Aktivieren des klassischen Modus kann nur durch zweimaliges Buchen mit demselben Dauer-Auf-Ausweis innerhalb des Gültigkeitszeitraumes erreicht werden.
  - Beim Aktivieren des klassischen Modus muss nach dem ersten Vorhalten des Ausweises mit der zweiten Buchung abgewartet werden, bis die Schaltzeit des Relais vorüber ist (eingestellte Dauer in der Action-Liste). Ebenso verhält es sich mit dem Deaktivieren des klassischen Modus, bei dem erst nach der Signalisierung des aktiven klassischen Modus die Rücknahme erfolgen kann.

Der Grund dafür ist, dass die Kommunikation mit dem Zylinder während dem geschalteten Relais nicht möglich ist und ein Ausweis erst danach wieder gelesen werden kann.

- Sofern der Ausweis zeitlich eingeschränkt gültig ist, ist das Aktivieren des klassischen Modus mit einem Dauer-Auf-Ausweis nur innerhalb des Gültigkeitszeitraumes des Ausweises möglich.
- Das Deaktivieren des klassischen Modus ist auch außerhalb des Gültigkeitszeitraumes des Dauer-Auf-Ausweises möglich, solange das Steuergerät in der Zwischenzeit keinen Neustart gemacht hat.
- Wenn der klassische Modus aktiv ist, wird bei jedem Ausweis – egal ob gültig oder nicht – durch die grüne LED signalisiert, dass die Tür geöffnet ist.
- Aufgrund der Tatsache, dass die Zylinder batteriebetrieben sind, können die LED-Signalisierungen nur nach einer Aktion am Zylinder erfolgen (Buchung durch Ausweis oder Betätigung des Zylinders).
- Nach dem Aktivieren des klassischen Modus und einem Neustart des Steuergerätes kann die Tür ohne vorherige Buchung noch einmal geöffnet werden, bevor das Relais in seinen Ursprungszustand zurückgesetzt wird (Relais wird ausgeschaltet). Dasselbe gilt für das erneute Aufspielen der Zutrittslisten (vor allem der Reader-Liste), da auch in diesem Fall die Zutrittskontrolle neu gestartet wird.
  - Hintergrund: Das Wiederherstellen des Ursprungszustandes erfolgt nach der ersten Aktion am Zylinder (Buchung durch Ausweis oder Betätigung des Zylinders). Das Wiederherstellen des Ursprungszustandes wird nach jedem Neustart des Steuergerätes durchgeführt.
  - Nach dem Wiederherstellen des Ursprungszustandes entsprechen die LED-Signalisierungen dem Zustand „Klassischer Modus nicht aktiv“.
- Der klassische Modus wird spätestens nach 12 Stunden automatisch deaktiviert, sofern er nicht zuvor durch den Anwender deaktiviert wird. Dadurch soll eine geöffnete Tür wieder verschlossen werden, wenn der Anwender vergessen hat den klassischen Modus zu deaktivieren.

## 4. Technische Daten KYO Cenloc

### KYO Cenloc V4.X

DE | TECHNISCHE DATEN

Gehäuse	Aufbau, Abmessungen (B x H x T)	Rack: 485 x 88 x 430 [mm] Wall: 300 x 400 x 128 [mm] Kit: 275 x 388 x 83 [mm]
	Gewicht (ohne Akku)	Rack: ca. 7,5kg Wall: ca. 7,5kg Kit: ca. 3,0 kg
System	Uhr	Echtzeituhr
Daten-Speicher	Flash	16 MB, 100.000 Schreibzyklen
	Speichererweiterung (optional)	SD-Card; max.2 GB
Anzeige, Tasten	LCD, 2 LEDs, 2 Tasten, kapazitiv. Touch	TFT: 480 x 320 Pixel, active area 73,4 x 49,0 mm mit LED-Backlight
Zutritt-Optionen	Tür-Anschlüsse	Sternförmiger Anschluss von bis zu 16 Türmodulen, max. 64 RS485 Busteilnehmer insg.
	Türmodul (optional)	1 Relais Wechsler, 30V AC, 30V DC, 2A, max. 60 W; 1 digitaler Eingang für Türüberwachung zum Anschluss an Taster oder Relais, gebrückt = Eingang aktiv; 1 x RS485; Versorgung Leser 15V, max. 350mA
	Anschluss Einbruchmeldeanlage (EMA) und Brandmeldeanlage (BMA)	6 Relais, 6 digitale Eingänge
Stromversorgung	Netzteil	15 V DC, 92W Gleichspannung integriert. Die Maximal-Leistung bei Versorgung der Leser und Türöffner muss vom Installateur berücksichtigt werden!
	Leistungsaufnahme	TBD
	Akku (optional)	Bleigel Akku: 12V, 7,2Ah - Gewicht: ca. 2,7kg
	Weiteres Netzteil für Türöffner	Auf Anfrage
	Uhr Pufferung	Lithium Batterie + Goldcap
Umgebungswerte	Umgebungstemperatur, Schutzart	-20 °C bis +60 °C (Netzteilleistung 100% bis 50°C), Wall IP65, Rack IP10
Software	Konfigurationsprogramm	Setupprogramm (Datafox-Studio) zum Konfigurieren ohne Programmieraufwand
	Kommunikationstools	http, DLL oder C-Source-Code zur Einbindung in die Anwendung
Modulerweiterungen	Für die Erweiterung um verschiedenste Funktionen wie Kommunikation, Ein- /Ausgänge, Sensoren,... stehen 3 Erweiterungsplätze für Auflötmodule Typ ML01 zur Verfügung. Es sind max. 32 digitale Eingänge für das Gerät möglich.	
Datenübertragung zu PC/Server	TCP/IP	TCP/IP-Betrieb mit integriertem TCP/IP-Stack, 10/100 Mbit
	USB	Micro-USB integriert
	WLAN (optional)	Wireless LAN Modul integriert, WLAN 802.11 bg und 802.11 n (nur 2,4GHz)
	GPRS (optional)	Online über GPRS, Mobilfunk-Modul Quadband 850 / 900 / 1800 / 1900 MHz
	RS485 (optional)	RS485 Bus
	Bluetooth (optional in Planung)	Bluetooth Modul integriert
Lesegeräteanschluss	RS232 extern (optional)	Anschluss von Barcodeleser, Magnetkartenleser etc. über Mini-DIN Stecker oder 4pol. Steckanschluss
Weitere Optionen	Teleskopauszug	Auszug für Rackversion für einfacheren Anschluss
	Wiegand Leser	Anschluss von bis zu 6 Wiegand Lesern mit 3 x LED, Buzzer und Sabotage-Anschluss
	Sabotage-Kontakt	Sabotagekontakt, der bei Öffnen des Gehäuses anspricht
	Individualisierung	Kundenspezifische Bedruckung von Frontplatte bzw. Schaltschranktür
	GPS-Empfänger / Receiver	50 Channels, GPS L1 frequency C/A, GALILEO Open Service L1

Technische Änderungen vorbehalten. Bei Zweifelsfällen bitte das aktuelle Prospekt mit den neusten technischen Daten unter [www.datafox.de](http://www.datafox.de) laden.

## 5. Index

### A

Akku 42

### B

Bios 21

### D

DHCP 36

Digitale Eingänge 43

Display 13

DNS 36

### E

EMA 93, 97

EVO 73

### F

Falscher 71

Feiertagssteuerung ZK 55

### I

Installationsvoraussetzungen 4

### K

Kommunikation 23

Umschalten 23

### O

Office-Mode 131, 133

Office-Mode-1 131

Office-Mode-2 133

Online Zutritt 103, 114, 115

### S

Spannungsversorgung 41

POE 41

### T

Tabellenbeschreibung 101

TCP/IP 29, 136

### U

USB 23, 25

USV 5

### W

WLAN 32, 33, 34

### Z

Zeitsteuerung 55

Zutritt 102

Statusmeldungen 92

Tabellenbeschreibung 58

Zutrittskontrolle 55, 105