



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

Handbuch Datafox EVO 2.8 Pure

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
02.01.2014	Alle	Neuaufgabe des Handbuches auf Versionstand 04.03.01.xx Integration der Evoline
07.03.2014	ZK, Kommunikation	Ergänzung der Kapitel ZK und Kommunikation
06.06.2015	Alle notwendigen	Anpassung an die FW 04.03.04
27.11.2015	Alle Kap. 4.3	Anpassung an die FW 04.03.05 Neues Befestigungsblech Hinweise IP54 und Montage
13.05.2016	SMS	Kapitel nachgepflegt
03.06.2016	Alle notwendigen	Anpassung an 04.03.06
14.12.2016	Alle notwendigen	Anpassung an 04.03.07
10.02.2017	Alle Notwendigen ZK-Plus Leser	Anpassung an 04.03.09 Neu im Kapitel ZK
02.11.2017	Hinweise POE	Bilder und Hinweise für die Spannungsversorgung über POE
18.04.2018	5.2.1	Hinweise für Touch
18.07.2018	Allgemeine Hardwareinformationen	Geräteinformationen
02.08.2019		Diverse Ergänzungen
01.11.2019	Alle notwendigen	Anpassung an 04.03.13
10.07.2020	Alle notwendigen	Anpassung an Software 04.03.15.xx
08.09.2022	Alle notwendigen	Anpassung an Software 04.03.17.xx
14.09.2023	Alle notwendigen	Anpassung an Software 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 zu- sammen eingesetzt werden)	ZZ. Versionsnummer (Funktionser-weite- rung)	Build Fehlerbeseitigung (mit ei- ner neuen Version wird die Build-Nr. auf Null gesetzt)
z. B. AE-MasterIV	04.	03.	04.	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.

Gültigkeit

Firmware, Gültigkeit: 04.03.17.xx

Studio und DLL: 04.03.19.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 unter Download zur Verfügung.

Inhalt

1.	Zu Ihrer Sicherheit	1
2.	Einleitung	2
2.1.	Aufbau des Handbuchs	2
2.2.	Einschränkung der Gewährleistung	2
2.3.	Typografie des Handbuchs	3
2.4.	Wichtige allgemeine Hinweise	3
3.	Bestimmungsgemäßer Gebrauch und Umweltschutz	5
3.1.	Vorschriften und Hinweise	5
3.2.	Stromversorgung	5
3.3.	Umwelteinflüsse	5
3.4.	Montage im Außenbereich	6
3.5.	Schutzart	6
3.5.1.	Temperatur	7
3.6.	Reparatur	7
3.7.	Reinigung	8
3.8.	Sonstige Hinweise	9
3.9.	Entsorgung	10
4.	Systemvoraussetzungen / Hardware	11
4.1.	Systemaufbau	11
4.2.	Installationsvoraussetzungen für den Betrieb der Datafox-Geräte	12
4.3.	Allgemeine Hardwareinformationen	13
4.3.1.	Hardware Ausstattung	13
4.3.2.	Verhalten bei Stromausfall	13
4.3.3.	USV	13
4.4.	Kompatibilität	14
4.4.1.	Das Firmwaredateiarchiv (*.dfz)	14
4.4.2.	Datafox-Geräte und Geräte-Firmware	14
4.4.3.	Geräte-Firmware und Geräte-Setup	14
4.4.4.	Geräte-Firmware und Kommunikations-DLL	15
4.4.5.	Kommunikations-DLL und DatafoxStudioIV	15
4.4.6.	DatafoxStudioIV und Geräte-Setup	15
4.4.7.	Update / Downgrade	16
5.	Gerät	17
5.1.	Inbetriebnahme	17
5.2.	Leitfaden zur Inbetriebnahme	18
5.2.1.	Einrichtung des EVO 2.8 Pure	18
5.2.2.	Installation des EVO 2.8 Pure	18
5.2.3.	Fehlersuche bei der Inbetriebnahme des EVO 2.8 Pure	18
5.3.	Bedienung und Anzeigeelemente des Evo 2.8 Pure	19
5.3.1.	Aufbau und Bedienung des EVO 2.8 Pure	19
5.3.2.	Display und Bios des EVO-Line 2.8 Pure	20
5.3.2.1.	Aufbau Display Normalanzeige	20
5.3.2.2.	Aufbau Display EVO 2.8 Pure im Bios-Menü	21
5.3.2.3.	Bios-Menü Einstellung WLAN	25
5.3.3.	Displaydesigner	28
5.3.3.1.	Farbeinstellung für die Anzeigen im EVO 4.3 / 4.6 / 2.8 / 3.5 / 5.0	29
5.3.3.2.	Standardeinstellungen	29
5.3.3.3.	Funktionstasten im Display des EVO 4.3 / 4.6 / 2.8 / 3.5 / 5.0 anzeigen	30
5.3.3.4.	Bilder für Funktionstasten des EVO 4.3 / 4.6 / 2.8 / 3.5 / 5.0 hochladen	30
5.3.3.5.	Zusätzliche Bilder übertragen	31
5.3.3.6.	Bild für das Fingerprintmenü hochladen	31

5.3.3.7.	Bilder für die Datenspeicherung hinterlegen	31
5.3.3.8.	Tastaturgrafik und Touchkonfiguration des EVO 4.6 FlexKey und EVO 5.0	33
5.3.3.9.	Bilder in Eingabefeldern anzeigen	33
5.3.3.10.	Designbeispiele im Designer enthalten	35
5.4.	Montage des EVO2.8/3.5/5.0 Pure Terminal	36
5.4.1.	Montagehöhe des EVO 2.8/3.5/5.0	36
5.4.2.	Alle Maßangaben für das EVO 2.8/3.5/5.0 Terminal	37
5.5.	Anschluss des EVO2.8 /3.5/5.0/ Pure Terminals	38
5.5.1.	Steckerbelegung.....	38
5.5.2.	Spannungsversorgung des EVO 2.8 / 3.5 /5.0 / Pure.....	39
5.6.	Spannungsversorgung über POE.....	39
5.6.1.	Wichtige Hinweise für die Nutzung von POE	39
5.7.	Modulbaugruppen für Geräte der Hardware V4.....	42
5.7.1.	Beschreibung der verschiedenen Erweiterungsmodule.....	42
5.7.2.	Bestückung von Modulen aus Gerät lesen.....	43
5.7.3.	Wichtige Modulinformationen vom Gerät auslesen	45
5.7.4.	Anschluss der einzelnen Modulbaugruppen.....	46
5.7.4.1.	Analogeingänge, 4 mal analog IN	47
5.7.4.2.	2 mal digital Out.....	48
5.7.4.3.	1 mal digital Out 1x digital IN	48
5.7.4.4.	4 mal digital IN.....	48
5.7.4.5.	4 mal digital OUT aktiv-Low (Masse geschaltet)	49
5.7.4.6.	4 mal digital OUT aktiv-Hi (Plus geschaltet)	49
5.7.4.7.	RS-485 Bus für ZK.....	50
5.8.	Kommunikationsarten der V4 Geräte	51
5.8.1.	Kommunikation der V4 Geräte über USB	51
5.8.1.1.	Automatische Erkennung über USB für V4 Terminals	52
5.8.1.2.	USB Treiberinstallation für Datafox Geräte HW V4	53
5.8.2.	Kommunikation über USB-Stick (Host)	56
5.8.2.1.	Fehlermeldungen bei USB-Stick (Host)	57
5.8.3.	Kommunikation über TCP / IP.....	58
5.8.3.1.	Kommunikation TCP / IP über LAN.....	59
5.8.3.2.	Kommunikation TCP / IP über WLAN	60
5.8.3.3.	M111_WLAN ESP32-c3 ML01 (wLAN-Modul DF-WL03).....	61
5.8.3.4.	Texas Instruments TI-CC3135 (Generation 2)	62
5.8.3.5.	Redpine (Generation 1)	63
5.8.3.6.	Einstellen der WLAN Parameter	64
5.8.3.7.	Verbindung der Terminals via TCP/IP DNS / DHCP	65
5.8.4.	Kommunikation der V4 Terminals über RS485	67
5.8.4.1.	Anschluss RS485 zum PC.....	67
5.8.4.2.	Anschluss EVO Terminal an RS485 über Comserver Lantronix.....	68
5.8.5.	Kommunikation über Mobilfunk.....	70
5.8.5.1.	Statusmeldungen für Mobilfunk am Display	71
5.8.6.	Kommunikation per SMS	72
5.8.6.1.	SMS versenden	72
5.8.6.2.	SMS empfangen.....	73
5.9.	Anschluss der Zutrittskontrolle	76
5.9.1.	Konfiguration der ZK / Übersicht.....	76
5.9.1.1.	Beschreibung der Tabellen für die Zutrittskontrolle 2	79
5.9.2.	Zutrittskontrolle II mit EVO Intera	82
5.9.2.1.	Anschluss der EVO Intera.....	84
5.9.3.	Zutrittskontrolle II mit EVO Agera.....	85
5.9.3.1.	Aufbau der Anzeigen und Bedienung.....	85
5.9.3.2.	Anzeigen für den ZK-Status.....	86
5.9.3.3.	Anzeigen einer PIN-Tastatur.....	86
5.9.3.4.	Fehlerausgaben.....	86

5.9.3.5.	Bios-Menü	87
5.9.3.6.	Allgemeine Konfiguration	87
5.9.3.7.	Display Konfiguration	88
5.9.3.8.	Bus Konfiguration	88
5.9.3.9.	Einstellen der Bus - Adresse	88
5.9.3.10.	Aktivierung des Bus - Abschlusswiderstands	88
5.9.3.11.	Anschluss des Agera	89
5.9.4.	Zutrittskontrolle II mit PHG-Modulen	93
5.9.4.1.	Anschluss der PHG-Leser	95
5.9.4.2.	Konfiguration	102
5.9.5.	Zutrittskontrolle II mit TS-Lesern	104
5.9.5.1.	Aufbau und Installationsvarianten	105
5.9.5.2.	Anschluss der TS-Leser	111
5.9.6.	Hinweise für den Elektriker zur Installation der Zutrittskontrolle	114
5.9.6.1.	Busverkabelung Sternförmig	114
5.9.7.	Berechnungsvorschrift für die Spannungsversorgung der ZK-Module	116
5.9.7.1.	Leitungslängen für PHG und EVO Intera	117
5.9.8.	Onlinefunktionen der Zutrittskontrolle	118
5.9.8.1.	Online über HTTP-Anbindung	118
5.9.8.2.	Online über DLL-Anbindung	121
5.9.9.	Funktionserweiterung für die Zutrittskontrolle 2	122
5.9.9.1.	Allgemeine Informationen	122
5.9.9.2.	Beispiele	122
5.9.9.3.	Tabelle <i>Time</i>	123
5.9.9.4.	Beschreibung der Tabelle „Action2“	127
5.9.9.5.	Weitere Funktionen für ZK	128
5.9.9.6.	Liste Presence	129
5.9.10.	Anbindung EMA (Einbruchmeldeanlage)	130
5.9.10.1.	Konfigurieren der EMA in der Zutrittskontrolle	130
5.9.10.2.	Relais und digitale Eingänge zur Steuerung (Type 2)	131
5.9.10.3.	Definition der Codes zum Ein- und Ausschalten (Type 3)	132
5.9.10.4.	Zuordnung der Leser zu EMA-Bereichen (Type 4)	133
5.9.10.5.	Ausweise zur EMA-Schaltung berechtigen	134
5.9.10.6.	Statuscodes	135
5.9.10.7.	Aktivierungsablauf im Controller	136
5.9.11.	Statusmeldungen der Zutrittskontrolle	138
5.9.12.	Statusanzeige der Zutrittsmodule über LEDs	143
5.9.13.	Funktionen für ZK und U&Z	144
5.9.13.1.	Aufbaubeispiel	144
5.9.13.2.	Inbetriebnahme der Schließzylinder	147
5.9.13.3.	Montage und Demontage der Zylinder	147
5.9.13.4.	Einrichten des Funknetzwerkes	148
5.9.13.5.	Batteriewechsel / Status / Lebensdauer	149
5.9.13.6.	Wechseln der ZK-Master ID / Knob Active Time	150
5.9.13.7.	Optische und akustische Signale des U&Z Schließzylinders	151
5.9.13.8.	Optische und akustische Signale des U&Z Türdrückers	152
5.9.13.9.	Zurücksetzen des U&Z Schließzylinders	152
5.9.13.10.	Hinweise zum Service Key	153
5.9.13.11.	Unterstützte Transponderverfahren und Einschränkungen	154
5.9.13.12.	Servicekey beschädigt / verloren	155
5.9.13.13.	Servicekey ersetzen	155
5.9.13.14.	Technische Daten des Funkmoduls	155
5.9.14.	Dauer-Öffnung bei Uhlmann&Zacher Funkbeschlägen	156
5.9.15.	U&Z-Dauer-Öffnung einer Tür (Variante 1 – Sicherer Betriebsmodus)	156
5.9.15.1.	Aktivieren der Daueröffnung	156
5.9.15.2.	Bedienung während Dauer-Öffnung	156

5.9.15.3.	Rücknahme einer Dauer-Öffnung	157
5.9.15.4.	Zusammenfassung	157
5.9.16.	U&Z-Dauer-Öffnung einer Tür (Variante 2 – Klassischer Modus).....	158
5.9.16.1.	Daueröffnung mithilfe des klassischen Modus	158
5.9.16.2.	Einrichten der Daueröffnung mithilfe des klassischen Modus	158
5.9.16.3.	LED- und Buzzer-Signalisierungen des Zylinders im klassischen Modus.....	159
5.9.17.	Bedienung /Aktivierung-Deaktivierung des Office-Mode	160
5.9.17.1.	Aktivierung.....	160
5.9.17.2.	Deaktivierung.....	160
5.9.17.3.	Hinweise	161
5.10.	Transponderleser	162
5.11.	Data on Card	163
5.11.1.	Allgemeine Informationen	163
5.11.2.	Einrichtung Data on Card.....	164
5.12.	Barcode Leser für V4 Terminals	168
5.13.	Fingerscanner, EVO	170
5.13.1.	Menüseite Finger prüfen	171
5.13.2.	Menüseite Finger „Einlernen“	171
5.13.3.	Menüseite „Trainieren“	172
5.13.4.	Menüseite „Löschen“	174
5.13.5.	Menüseite „Beenden“	174
5.13.6.	Hinweise zur Verwendung des Fingerprint-Flächensensors.....	174
5.13.6.1.	Hints for using the fingerprint area sensor	174
5.14.	Fingerscanner mit Zeilensensor	178
5.14.1.	Bedienung Fingerscanner	178
5.14.2.	Allgemeine Informationen	179
5.14.3.	Einlernen	181
5.14.4.	Verfahren.....	182
5.14.5.	Ablaufvarianten.....	183
5.14.6.	Technische Daten Fingerprint-Modul	184
5.15.	Fingerprint, Informationen und Vergleich.....	184
5.16.	Weitere Funktionen	187
5.16.1.	Einstellung Näherungs- & Umgebungslicht-Sensor im Studio	187
6.	Technische Daten EVO 2.8 /3.5 /5.0 Pure	188
6.1.	Module Kommunikation	189
6.2.	Module Zutritt.....	189
6.3.	Module I/O (MDE).....	189
6.4.	Module verschieden	189
7.	FAQ & Fragen und Antworten	189
8.	Index	190

1. Zu Ihrer Sicherheit

Sicherheitshinweise für den Umgang mit den Datafox Produkten



Das EVO 2.8 Pure 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. Einleitung

Datafox Datenterminals wurden speziell für die Anforderungen an eine moderne Personalzeiterfassung entwickelt, deren Nutzer hohe Ansprüche an ein flexibles und edles Design stellen. Durch das Datafox Embedded-Konzept wird zusätzlich auch die Funktion der Zutrittskontrolle abgedeckt. Alle relevanten Daten können mit neuester Technik erfasst und sofort an die Auswertesoftware übertragen werden. Abrechnungen, Kalkulationen oder andere Auswertungen können zeitnah erfolgen, Prozesse gezielt verfolgt und gesteuert werden. Dies spart Zeit und sorgt für die notwendige Datenqualität und Datenaktualität.

Datafox Datenterminals basieren auf dem Datafox Embedded-System, welches ausgerüstet ist mit modernster Technik für die Datenerfassung und natürlich auch für die Datenübertragung. Ihre Eingaben erledigen Sie bequem über Tastatur, Touch Display, RFID oder per Barcode. Das Gerät ist erhältlich mit: Fingerprint, GPS, GSM, GPRS, USB, etc. Es erfüllt alle Voraussetzungen, um absolut flexibel eingesetzt zu werden. Nicht nur zur Personal- und Auftragszeiterfassung sondern für deutlich mehr Anwendungen. Das bedeutet einen echten Mehrwert. Die leistungsfähigen Tools DatafoxStudioIV und DLL ermöglichen eine schnelle und einfache Integration in beliebige IT-Lösungen. Durch die Skalierbarkeit stehen vielfältige Optionen zur Verfügung. Hierbei wählen und bezahlen Sie nur die, die Sie auch wirklich brauchen.

2.1. Aufbau des Handbuches

Das Handbuch besteht aus einer Änderungshistorie, einem allgemeinen Teil mit Sicherheitshinweisen, der Einleitung, den Systemvoraussetzungen sowie Informationen zum Systemaufbau.

Dem allgemeinen Teil folgt der Hauptteil des Handbuches. Er besteht aus dem Kapitel „Produktbeschreibung“ Gerät“. Hier werden die gerätespezifischen Komponenten beschrieben. Ebenso werden die Funktionen des Gerätes beschrieben, d. h. was kann das Gerät.

Im Schlussteil des Handbuches finden Sie die technischen Daten zum Gerät sowie eine Begriffsklärung (Glossar), die dem einheitlichen Verständnis zwischen Anwender und Hersteller dienen soll.

2.2. Einschränkung der Gewährleistung

Alle Einrichter sind dafür verantwortlich, dass das Gerät und dessen Zubehör nur unter Beachtung der geltenden Gesetze, Normen und Richtlinien bestimmungsgemäß eingesetzt werden.

Alle Angaben in diesem Handbuch wurden sorgfältig geprüft. Trotzdem sind Fehler nicht auszuschließen. Es können somit weder eine Garantie noch die juristische Verantwortung für Konsequenzen, die auf Fehler dieses Handbuches zurückzuführen sind, übernommen werden. Natürlich sind wir für Hinweise auf Fehler jederzeit dankbar. Änderungen im Sinne des technischen Fortschritts behalten wir uns vor. Es gelten unsere allgemeinen Geschäftsbedingungen.



Hinweis:

Die Datafox-Geräte bieten durch das DatafoxStudioIV sehr viele Funktionen und Funktionskombinationen, wodurch es bei Updates nicht möglich ist, alle Funktionen und Funktionskombinationen zu testen. Dies gilt insbesondere nicht mit allen von Ihnen als Kunden erstellten Setups. Bevor Sie das Update auf Ihre Geräte übernehmen, stellen Sie durch Tests bitte sicher, dass Ihr individuelles Setup fehlerfrei arbeitet. Wenn Sie ein Problem feststellen, teilen Sie uns das bitte umgehend mit. Wir werden uns dann kurzfristig um die Klärung des Sachverhaltes kümmern.

2.3. Typografie des Handbuches

FW	Abkürzung für Firmware (Software im Gerät)
SW	Abkürzung für Software
HW	Abkürzung für Hardware
GV	Abkürzung für Globale Variable
<Name;Software Version.pdf>	Dateinamen und Pfadangaben



Hinweis:

Hier erhalten Sie nützliche Hinweise, die Ihnen helfen bei der Installation, Konfiguration und Inbetriebnahme mögliche Fehler zu vermeiden.



Achtung:

Hier werden Hinweise gegeben, die unbedingt einzuhalten sind. Andernfalls kommt es zu Fehlfunktionen des Systems.

2.4. Wichtige allgemeine Hinweise



Achtung:

Setzen Sie die Geräte nur bestimmungsgemäß und unter Beachtung der Montage-, Inbetriebnahme- und Bedienungsanleitung ein. Montage und Inbetriebnahme dürfen nur von autorisiertem Fachpersonal vorgenommen werden.

Technische Änderungen vorbehalten.



Achtung:

Aufgrund der technischen Weiterentwicklung können Abbildungen, Funktionsschritte, Abläufe und technische Daten geringfügig abweichen.

Das Datafox Gerät wurde mit dem Ziel entwickelt, ein flexibles und leicht zu integrierendes Terminal zur Datenerfassung zu schaffen, welches in verschiedensten Einsatzgebieten verwendet werden kann. Das Gerät ist robust und leicht zu bedienen. Durch das PC-Setupprogramm DatafoxStudioIV sparen Sie Zeit, da das Gerät schnell und leicht für die Aufgabenstellung konfiguriert wird.

Die vielfältigen optionalen Ausstattungsmöglichkeiten der Datafox-Geräte wie z.B. Barcodeleser, Transponderleser, digitale Eingänge etc. ermöglichen den variablen Einsatz für:

PZE	- Personalzeiterfassung
AZE	- Auftragszeiterfassung
BDE	- Betriebsdatenerfassung (I/O-Verarbeitung)
ZK	- Zutrittskontrolle
FZDE	- Fahrzeugdatenerfassung / Telematik

Dieses Handbuch beschreibt allgemein die Erstellung von Setups mit dem Setupprogramm DatafoxStudioIV ohne dabei auf spezifische Einsatzgebiete einzugehen. Dabei wird auf mögliche Stolpersteine hingewiesen.

Dieses Handbuch beschreibt die Funktionalität des EVO 2.8 Pure und geht dabei auf Besonderheiten ein. Es werden dabei z.B. der Aufbau, die Bedienung und die Ausstattung des Gerätes beschrieben.

Um das Verhalten des Gerätes fest zu legen, muss ein Setup erstellt werden. Dafür wurde eigens das DatafoxStudioIV entwickelt.

Mit etwas Übung ist es möglich, in einer halben Stunde eine komplette Erfassung für den EVO 2.8 Pure anzulegen. Sollten Funktionen benötigt werden die nicht vorhanden sind, sollten wir darüber sprechen.

**Hinweis:**

Benötigen Sie Unterstützung beim Anlegen von Setups, bieten wir Ihnen das gerne in Form von Dienstleistung an. Durch unsere umfangreiche Erfahrung im Umgang mit dem Setup sind wir sehr schnell in der Erstellung von Setups und können dadurch auch wertvolle Hinweise geben um Ihr Setup noch leistungsfähiger zu gestalten, dass die Eingabe am Gerät sicher und schnell erfolgen kann.

**Hinweis:**

Die Datafox-Geräte bieten durch das DatafoxStudioIV sehr viele Funktionen und Funktionskombinationen, wodurch es bei Updates nicht möglich ist, alle Funktionen und Funktionskombinationen zu testen. Dies geht insbesondere nicht mit allen von Ihnen als Kunden erstellten Setups. Bevor Sie das Update auf Ihre Geräte übernehmen, stellen Sie durch Tests bitte sicher, dass Ihr individuelles Setup fehlerfrei arbeitet. Sollten Sie nach eingehender Prüfung Ihres Setups noch Fehler feststellen, teilen Sie uns das bitte umgehend mit. Wir werden den Fehler dann kurzfristig beheben.

3. Bestimmungsgemäßer Gebrauch und Umweltschutz

3.1. Vorschriften und Hinweise

Es wurde nach heutigem Stand der Technik und der Möglichkeiten sichergestellt, dass das Gerät die technischen und gesetzlichen Vorschriften und Sicherheitsstandards erfüllt. Dennoch sind Störungen auf Grund von Beeinträchtigungen durch andere Geräte möglich.

Beachten Sie bei der Nutzung des Gerätes stets die örtlichen Vorschriften und Regelungen.

3.2. Stromversorgung

Das Gerät darf extern mit einer Stromquelle mit begrenzter Leistung, entsprechend EN 60950-1 betrieben werden.

Anschlussspannung der MasterIV-Geräte: 12 bis 24 Volt DC

Sofern die Geräte Akkus enthalten, beachten sie die jeweiligen Hinweise im Kapitel „Akku“.



Achtung:

Bei Nichteinhaltung können das Gerät bzw. der Akku (sofern vorhanden) beschädigt oder zerstört werden!

3.3. Umwelteinflüsse

Extreme Umwelteinflüsse können das Gerät beschädigen oder zerstören und sind daher zu vermeiden. Dazu gehören Feuer, extreme Sonneneinstrahlung, Wasser, extreme Kälte und extreme Hitze. Beachten Sie bitte das jeweilige Typenschild des Gerätes.

3.4. Montage im Außenbereich

3.5. Schutzart

Schutzart

Das Terminal EVO 2.8 Pure hat frontseitig IP54.

Rückseitig ist in Bezug auf die IP-Klasse nur die Kabelzuführung bzw. der Anschlussbereich eine Einschränkung.

Der Anschlussbereich ist zur Geräterückwand nach oben gesetzt, so dass kein Wasser, das von oben kommt (z.B. Regen), eindringen könnte.

Lediglich Strahlwasser von unten wäre ein Problem.

Sollten Zusatzbedingungen über die normale Witterung hinaus dazu führen, dass Strahlwasser von unten kommen kann, können die Terminals bei der Montage zur Wand hin abgedichtet werden.

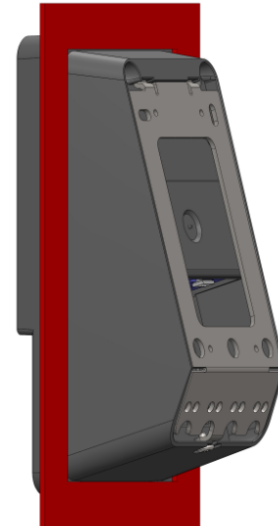
Bei den EVO-Terminals bietet sich an, die Geräte auf dem Absatz der Frontschale zu montieren.

Damit wäre das komplette Geräte-Rückteil mit den Anschlüssen versenkt und im nicht zugänglichen Bereich.

Um eine solche Montage zu ermöglichen, muss bauseits eine Montageebene zur Verfügung gestellt werden.

Hier bieten sich z.B. Unterputzkästen mit Frontplatte an.

Bei Klingelanlagen/Briefkastenanlagen/Schranken sind in der Regel bereits Montageplatten vorhanden, die dafür genutzt werden können.



Ansicht versenkter Einbau in einer Frontplatte / Montageplatte.

3.5.1. Temperatur

Das EVO 2.8 Pure hat einen zugelassenen Temperaturbereich von – 20°C bis + 60°C.

Eine Heizung ist auch für den Einsatz im Außenbereich nicht notwendig.

Durch die Eigenwärme von Elektronik und Netzteil sind auch bei Außentemperaturen kleiner -20°C die Temperaturen im Gerät höher.

Schwitzwasser tritt nur auf, wenn ein kalter Gegenstand ins Warme kommt und wäre damit nur bei Geräten ein Thema, die mobil betrieben werden.

Sowohl in Bezug auf das Thema Temperatur, als auch Schwitzwasser ist es zu empfehlen, Geräte die im Außenbereich genutzt werden, immer durchlaufen zulassen.

3.6. Reparatur

Die Datafox Geräte sind bis auf den Austausch wartungsfrei. Die Geräte die über ein Garantie-Siegel verfügen dürfen nur von autorisiertem Fachpersonal geöffnet werden. Kontaktieren Sie im Falle eines Defektes Ihren Fachhändler oder die Datafox Service-Hotline. Liegt ein definitiver Defekt vor, können Sie das Gerät auch direkt zu Datafox einsenden.

Zum einsenden verwenden Sie bitte den Reparatur-Begleitschein.

https://www.datafox.de/reparaturen.de.html?file=files/Datafox_Devices/PDF/Support/Datafox_Reparaturbegleitformular_V3_D-EN_2018.01.05.pdf

<https://www.datafox.de/reparaturen.de.html>

3.7. Reinigung



Zum Entfernen von Verunreinigungen dürfen auf keinen Fall Scheuermilch oder ätzende Reinigungsmittel verwendet werden. Insbesondere die Displays, als auch die Tastatur und Fingerprintmodule sind vorsichtig zu reinigen.

Zulässig sind feuchte Tücher mit:

- Wasser
- Seifenlauge
- Glasreiniger
- Sagrotan
- antifact® N liquid (Desinfektionsmittel für Geräte im medizinischen Bereich.)



3.8. Sonstige Hinweise

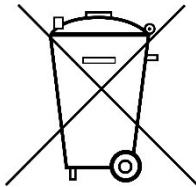
Setzen Sie das Gerät keinen starken magnetischen Feldern aus, insbesondere während des Betriebes. Die Steckplätze und Anschlüsse des Gerätes sind nur mit den jeweils dafür vorgesehenen Versorgungs- und Zusatzgeräten zu betreiben.

Achten Sie beim Transport des Gerätes auf eine sichere Lagerung. Als Fahrer eines Kraftfahrzeuges benutzen Sie das Gerät zu Ihrer eigenen Sicherheit nicht selbst während der Fahrt. Achten Sie auch darauf, dass technische Einrichtungen Ihres Fahrzeuges nicht durch das Gerät beeinträchtigt werden.

Um einen Missbrauch der SIM-Karte zu vermeiden, denken Sie bei Verlust oder Diebstahl des Gerätes daran, die SIM-Karte sofort sperren zu lassen.

3.9. Entsorgung

Beachten Sie unbedingt die örtlichen Vorschriften für die Entsorgung von Verpackungsmaterialien, verbrauchten Akkus / Batterien und ausgedienten Elektrogeräten. Dieses Produkt stimmt mit der EG-Richtlinie 2002/95/EG, deren Anhängen und dem Beschluss des Rates der EG zur Beschränkung der Nutzung von gefährlichen Stoffen in elektrischen und elektronischen Geräten überein. Das Gerät fällt unter das am 13. Februar 2003 in Kraft getretene und in der Bundesrepublik Deutschland am 18. August 2005 umgesetzte europäische Gesetz zur Vermeidung von Elektro- und Elektronikmüll (ElektroG).



Das Gerät darf nicht über den Hausmüll entsorgt werden!

Sie als Benutzer sind dafür verantwortlich, dass jeder Elektro- oder Elektronikmüll über die entsprechenden Stellen, zum Beispiel den Werkstoffhof, entsorgt wird. Das korrekte Entsorgen von Elektro- und Elektronikmüll schützt das menschliche Leben und die Umwelt.

Für mehr Informationen über die Entsorgung von Elektro- und Elektronikmüll wenden Sie sich bitte an die lokalen Stellen, wie Rathaus oder Müllentsorgungsunternehmen.

4. Systemvoraussetzungen / Hardware

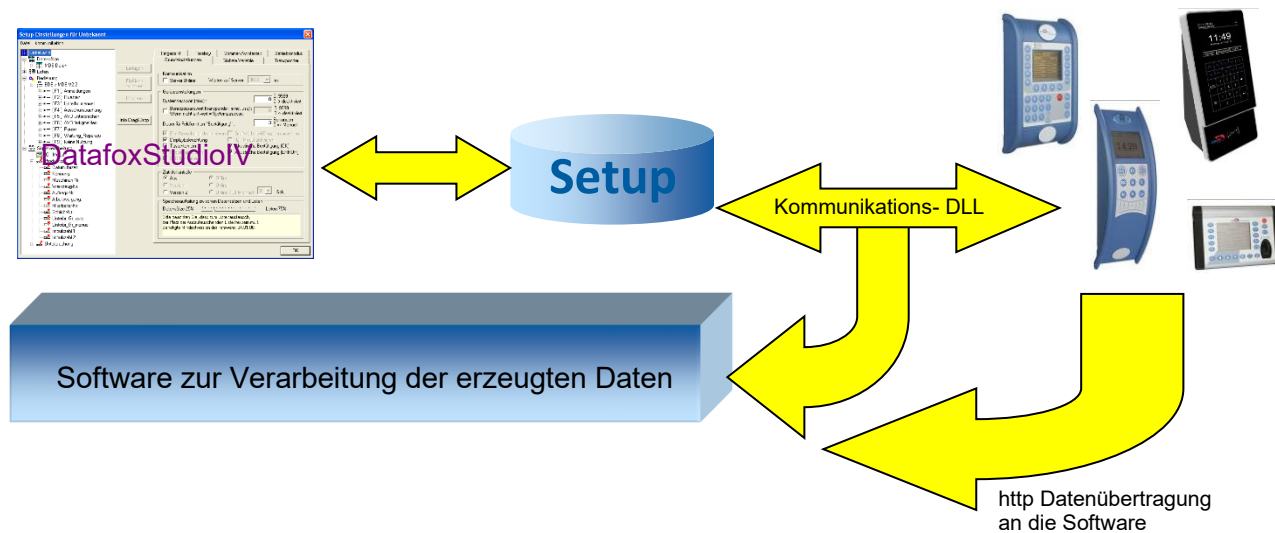
4.1. Systemaufbau

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



4.2. 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/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/kyo-cenloc/124401_Datafox_KYO_Cenloc_Rack_-_TKSS_Montageanleitung.pdf

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

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

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



Hinweis:

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

4.3. Allgemeine Hardwareinformationen

4.3.1. 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 überschieben. 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.

4.3.2. 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.

4.3.3. USV

Eine entsprechende USV für die Hardware V4 wird aktuell nicht angeboten.

Hier empfehlen wir, die Geräte mit einem POE Modul auszustatten, wenn eine „USV“ genutzt werden soll. Schließen Sie die Geräte dann über einen POE-Switch an und versorgen Sie den Switch über eine Standard USV.

4.4. 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

4.4.1. 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.

4.4.2. 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.

4.4.3. 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.

4.4.4. 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.

4.4.5. 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.

4.4.6. 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 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.

4.4.7. 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.

5. 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.

5.1. 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 (Netzteil einstecken) 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 EVO 2.8 Pure 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.

5.2. Leitfaden zur Inbetriebnahme

5.2.1. Einrichtung des EVO 2.8 Pure

Hier wird ein kurzer Leitfaden für die Inbetriebnahme gegeben, und die entsprechenden Links, wo dieses im Handbuch zu finden ist.

- ▶ Gerät mit der Stromversorgung verbinden
- ▶ Schnittstelle für die Kommunikation einstellen
- ▶ Setup des Gerätes einspielen
Siehe Handbuch „[DatafoxStudioIV](#)“

5.2.2. Installation des EVO 2.8 Pure

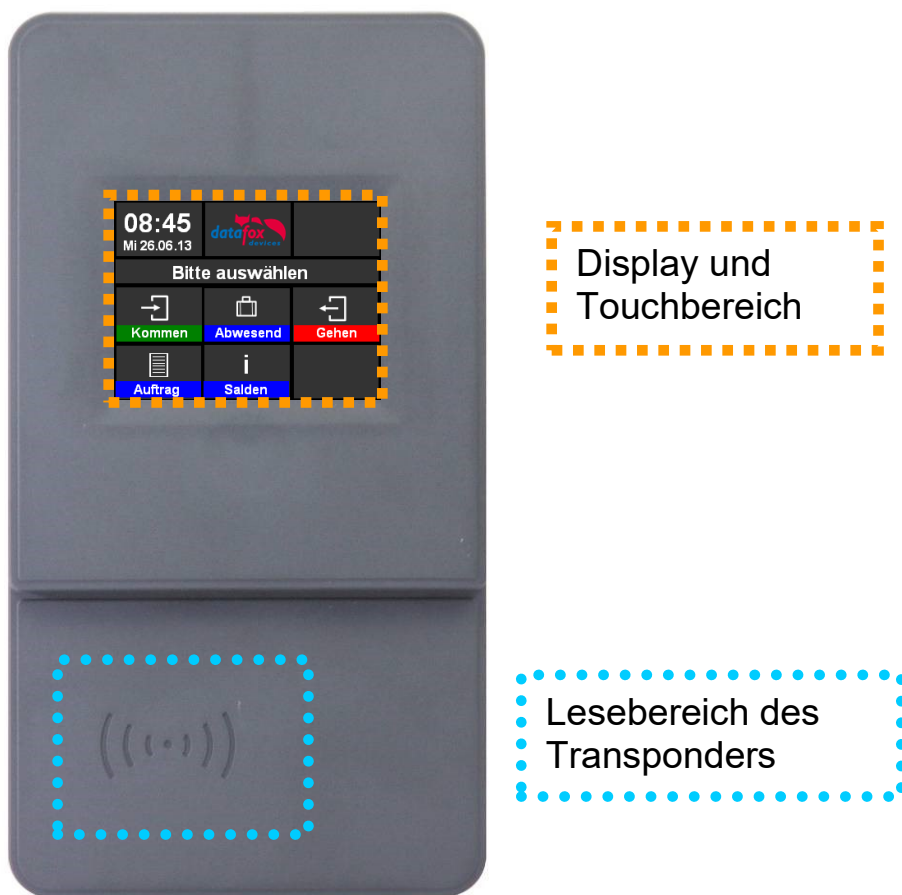
- ▶ Montage des Gerätes am Bestimmungsort
- ▶ Anschlüsse herstellen für:
 - Spannungsversorgung
 - Kommunikation:
 - [USB](#)
 - [TCP/IP \(HTTP\)](#)
 - [TCP/IP WLAN](#)
 - [GPRS/GSM](#)
 - [RS485](#)
 - Digitale Eingänge
 - Analoge Eingänge / MDE
 - [Zutrittskontrolle](#)
- ▶ Gerät fertig befestigen
- ▶ Einstellen der Hauptkommunikation

5.2.3. Fehlersuche bei der Inbetriebnahme des EVO 2.8 Pure

- ▶ Als Erstes schauen Sie bitte auf unserer Webseite in die FAQ
<http://www.datafox.de/faq-de.html>
- ▶ Kleine Tipps:
 - Verbindung zu Gerät lässt sich nicht über TCP/IP herstellen
 - IP im Gerät und der Anwendung (Studio) prüfen
 - Ping auf IP
 - Einstellung „Aktive Verbindung“ im Bios ? → auf nein umstellen
 - Einstellung „HTTP“ im Bios ? → auf nein umstellen

5.3. Bedienung und Anzeigeelemente des Evo 2.8 Pure

5.3.1. Aufbau und Bedienung des EVO 2.8 Pure



Das EVO 2.8 hat einen resistiven Touch. Das resistive Touchsensor-Folienpaket liegt vor dem Glas und reagiert auf Berührung.

Durch die Betätigung werden 2 leitfähige Schichten aufeinander gedrückt und der Punkt durch elektrische Messung ermittelt.

Wird das Touchfolienpaket beschädigt, kann es zu Unterbrechungen oder auch zu ungewollten Dauerbetätigungen kommen, so als wenn der Finger nicht vom Touch genommen wird.

In der Praxis wird z.B. festgestellt, dass Mitarbeiter den Touch mit dem Autoschlüssel betätigen. Diese führt in der Regel recht schnell zum Ausfall.



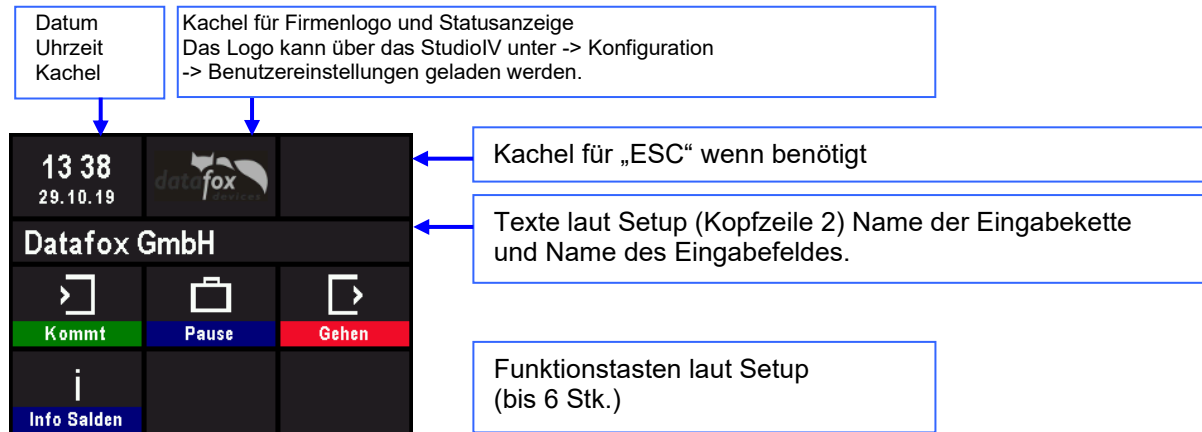
Achtung:



















Der resistive Touch darf nicht mit harten und kantigen oder scharfen Gegenständen belastet bzw. betätigt werden.

5.3.2. Display und Bios des EVO-Line 2.8 Pure

5.3.2.1. Aufbau Display Normalanzeige

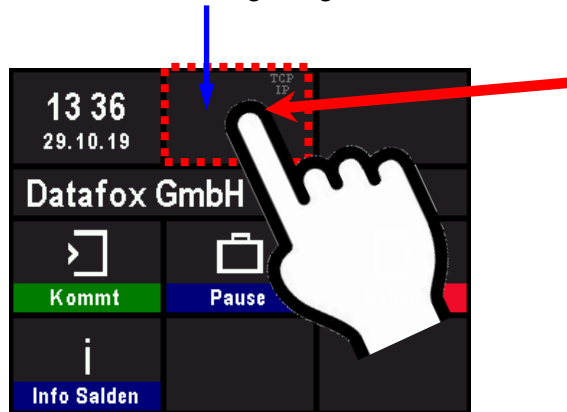
Die gesamte Displayfläche ist mit einem Touch versehen. Tippen Sie einfach mit dem Finger auf die jeweilige Kachel, welche Sie anwählen möchten.



- **Datum Uhrzeit** entspricht der Systemzeit des Gerätes, die auch für die Datensätze verwendet wird.
-  **Anzahl der Datensätze** im Speicher (Anzeige bis 99, danach 99+).
- **Kommunikationsfeld** mit Symbolen für:
-  **TCP /IP** Bei aktiver Kommunikation wird dieses Symbol eingeblendet, .
 - Wlan Kommunikation
 -  Wlan als Hauptkommunikation aktiviert
 -  Wlan verbunden
 -  Wlan Kommunikation gerade aktiv
 -  USB
 -  USB Host (Speichern der Daten auf USB - Stick)
 - GPRS mit Statusanzeige z.B. [33] siehe „Statusmeldungen am Display“.
 -  Mobilfunkmodem ist aus
 -  Mobilfunkmodem ist ein geschaltet, aber keine Verbindung zum Provider.
 -  Mobilfunkmodem ist eingeschaltet, Verbindung zum Provider besteht.
 - Mobilfunk (BG-96 und EG-95) mit Statusanzeige z.B.[33] siehe „Statusmeldungen am Display“.
 -  Mobilfunkmodem ist aus
 -  Mobilfunkmodem ist an, aber keine Verbindung zum Provider.
 -  Mobilfunkmodem ist an, Edge Verbindung zum Provider besteht.
 -  Mobilfunkmodem ist an, 3G Verbindung zum Provider besteht.
 -  Mobilfunkmodem ist an, LTE Verbindung zum Provider besteht
 -  Resistiv Touch „nicht betätigt“
 -  Resistiv Touch „betätigt“
- **Anzeige im Display**
 - Im Hauptmenü wird die Kopfzeile 2 des Setups angezeigt.
 - In Menüs und Eingabeketten werden die im Setup hinterlegten Kopfzeilen 3 und 4 angezeigt.
 - Während der Übertragung eines Setups oder Firmware-Updates, geht das Gerät in den Systemstopp und zeigt den Text „Systemstopp“ in diesem Fenster.

5.3.2.2. Aufbau Display EVO 2.8 Pure im Bios-Menü

In das Bios-Menü gelangt man, in dem die Kachel für Firmenlogo/Status 2 Sekunden gedrückt wird.



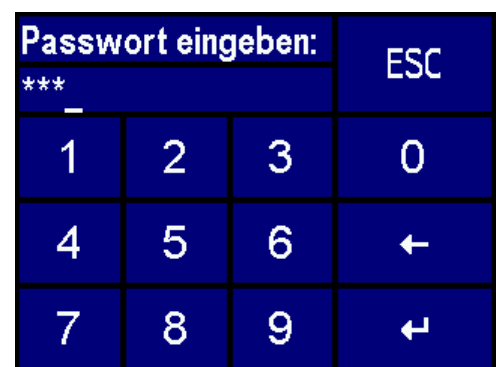
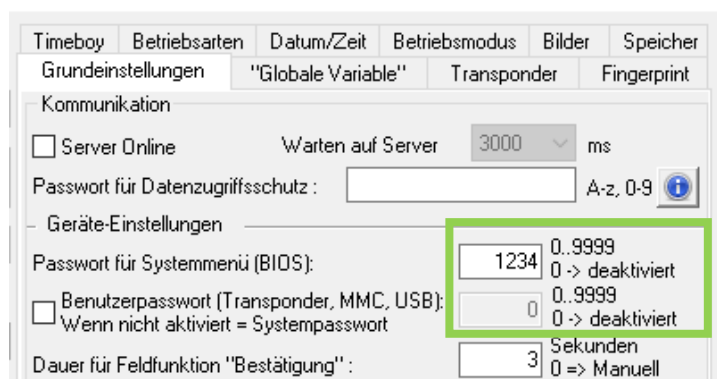
Anzeige der Status-Icons:

Tippen Sie kurz auf das Logo, um die Status-Icons anzuzeigen.

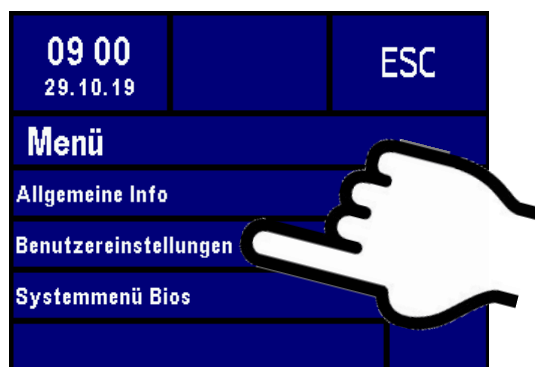
Sie können auch in den Benutzereinstellungen die Anzeige der Icons umstellen auf:

- Ständig anstatt des Logos
- Ständig in der „ESC“ Kachel
- Für 60 Sekunden anstatt des Logos
- Aus

Ist ein Bios- Passwort gesetzt, kann dies hier eingegeben werden.



Anzeige im Biosmenü:



Zum Auswählen der jeweiligen Menüs, einfach mit dem Finger darauf tippen.

Allgemeine Info:

- Firmware Info
- Transpondertest
- Speicherbelegung
- Signalstärke
- Provider
- Datenspeicher 3068kByte
- Listenspeicher 1028kByte

Die jeweiligen Untermenüs sollten selbsterklärend sein. Die jeweilige Anzeige richtet sich nach der Hardwareausstattung.

Systemmenü Bios:

09:38 29.10.19	ESC
Menü	
Firmware Info	^
System Info	
Kommunikation	v
Anzeige / Signallautstärke	

Die jeweiligen Untermenüs sollten selbsterklärend sein. Die jeweilige Anzeige richtet sich nach der Hardwareausstattung.

Kommunikation einstellen:

09:38 29.10.19	ESC
Menü	
Firmware Info	^
System Info	
Kommunikation	v
Anzeige / Signallautstärke	

09:39 29.10.19	ESC
Kommunikation	
Kommunikation unterbrechen?	
Bitte hier bestätigen.	

09:42 29.10.19	ESC
Kommunikation	
Schnittstelle LAN	^
Active-Mode Nein	
HTTP-Modus Nein	v
LAN-Parameter	

- Wählen Sie hier die Schnittstelle für die Hauptkommunikation aus.
- Parameter für active connection (Standard = nein)
- Parameter für http (Standard = nein)
- Einstellung der TCP/IP Parameter (IP-Adresse)

TCP / IP / DHCP - Einstellungen:

09:48 29.10.19	ESC
LAN-Parameter	
MAC E4-F7-A1-00-26-F4	^
DHCP Nein	
IP 192.168.1.109	v
Netmask 255.255.255.0	

Steht das Gerät auf DHCP (ja), können Sie die IP -Adresse nicht mehr per Hand ändern. Die vom Server zugewiesene IP wird Ihnen aber angezeigt.

TCP / IP - Einstellungen:

09:50 29.10.19	ESC
LAN-Parameter	
Gateway 192.168.1.1	^
Port 8000	
Meldezyklus (alive) 45	v

IP – einstellen

IP			ESC
192.168.001.109			
1	2	3	0
4	5	6	←
7	8	9	↶

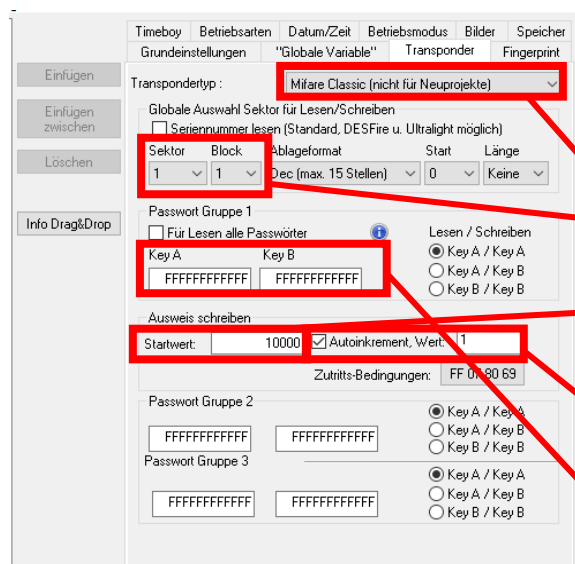
Transpondermenü

Die im Transpondermenü bestehenden Einstellungen können auch Setup eingestellt werden.



Name	Bedeutung
Typ	Typ des Transponderlesers
Version	Version des Transponderlesers
Schreibe Ausweise	Beginnt mit dem Schreiben
Inkrement	Autoinkrement
Wert	Startwert
Formatierung Sektor	aktiv = Sektor wird initialisiert deaktiv = Schon geschriebene Werte bleiben erhalten

Einige Einstellungen zum Schreiben der Ausweise müssen im Setup angepasst werden.



Name	Bedeutung
Transpondertyp	Hier muss der richtige Transpondertyp angegeben werden
Sektor und Block	In welchem Sektor und Block geschrieben/gelesen werden soll.
Startwert	Legt den Startwert der zu programmierenden Nummer fest
Autoinkrement	Wenn aktiviert, zählt den Programmierwert immer die entsprechende Anzahl hoch
Passwort	Das Passwort zum schreiben/lesen der Ausweise



Hinweis:

Wenn Ausweise mit Passwort geschrieben werden sollen, muss auf diesen vorher das Passwort programmiert werden.



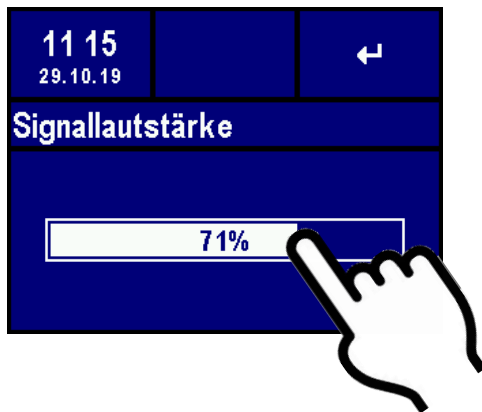
Achtung:

Im Setup müssen ein programmierbarer Transpondertyp und ein programmierbares Segment eingestellt sein. Bsp.:

- Hitag 2 → ab Segment 4
- Mifare Classic → ab Sector 0 Block 1

Ansonsten wird nur Typ und Version des Transponderlesers angezeigt.

Buzzerlautstärke:

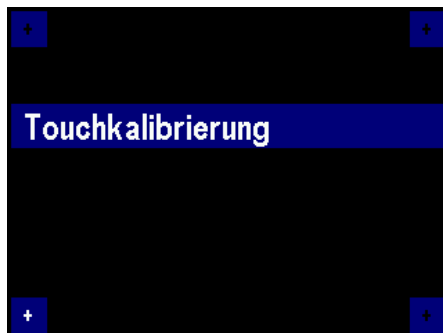


Dieses Menü finden Sie unter „Benutzereinstellungen“ → „Anzeige/Signallautstärke“.
→ „Signallautstärke“
Tippen Sie einfach auf den Balken in der Mitte, um die Lautstärke zu ändern,

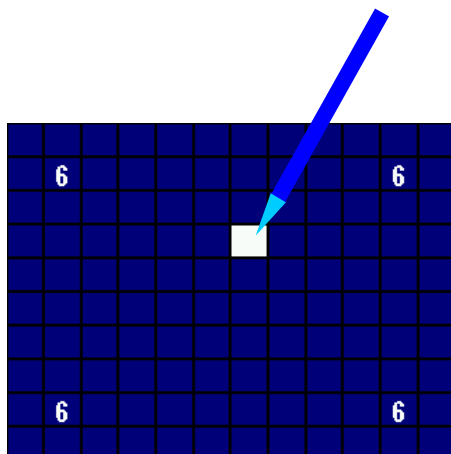
Touchkalibrierung:



Dieses Menü finden Sie unter „Benutzereinstellungen“ → „Touch“.



- 1.) Tippen Sie mit einem Bedienstift auf die Touchfläche. Das entsprechende Kreuz schalte die Farbe um.
- 2.) Fahren Sie nun mit dem Bedienstift möglichst genau auf das Kreuz.
- 3.) Erst beim Loslassen wird die jeweilige Ecke kalibriert



Um den Touch zu testen, fahren Sie einfach mit dem Bedienstift über das Display. Die jeweilige Kachel muss dann die Farbe zu weiß wechseln.

Wenn 7 Sekunden lang keine Bedienung erfolgt, wird der Kalibriertest automatisch beendet.

5.3.2.3. Bios-Menü Einstellung WLAN

Ab der Firmware 04.03.11 haben Sie die Möglichkeit die Einstellungen für die WLAN-Verbindung nicht nur mit dem DatafoxStudioIV vorzunehmen, sondern auch direkt am Gerät zu verändern.

In dem Bios-Menü „WLAN-Parameter“ können Sie die einzelnen Konfigurationen bearbeiten.



Hier sehen Sie mit welcher Konfig das Gerät sich aktuell verbindet.
Hier im Beispiel: „Datafox 2.4GHz“

Konfig Bearbeiten:

Als nächstes kann im dem Menüpunkt „Konfig. Bearbeiten“ die aktuell geladenen Konfiguration bearbeiten. Die einstellbaren Optionen entsprechen dem Netzwerkkonfiguration Abschnitt im Studio. Es kann zwischen DHCP und statischer IP Adresse gewechselt werden, als auch der Port angepasst werden. Zusätzlich gibt es hier die Möglichkeit eine Konfiguration als Standard zu definieren. Diese wird ausgewählt, falls die automatische Wahl der Konfiguration ausgestellt ist.

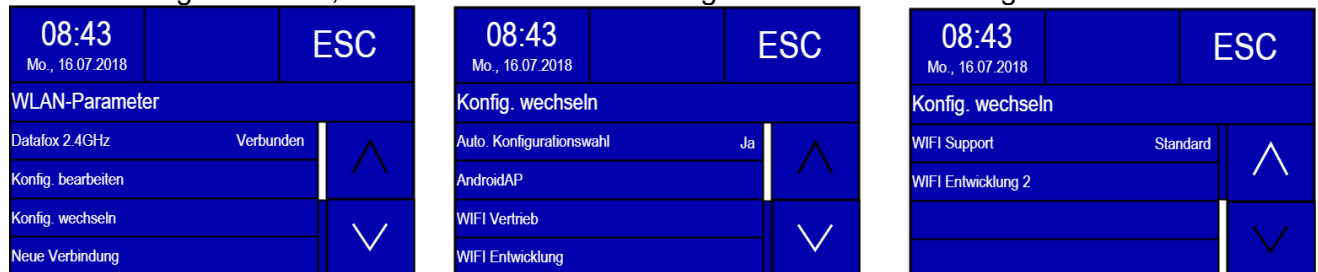
! Achtung: Diese Funktion wird nur bei EVO 2.8 Pure, 3.5 Pure, 3.5 Universal und 4.3 unterstützt.

Falls Änderungen vorgenommen wurden wird beim Verlassen des Menüs gefragt ob diese gespeichert werden sollen. Ja → speichert die Änderungen und verlässt das Menü. Nein → verlässt das Menü ohne die Änderungen zu Speichern. Durch ESC findet man sich wieder im Änderungsmenü, und kann die getroffenen Änderungen noch einmal ansehen.



Konfig. wechseln

Im Menüpunkt „Konfig. Wechseln“ kann zwischen Konfigurationen gewechselt werden. Des Weiteren kann hier die automatische Wahl der Konfiguration eingestellt werden. Wird hier ein Netzwerk ausgewählt, welches auch eine Verbindung zu einem Access Point herstellen kann ist jedoch nicht garantiert, das dieses Netz beim Verlassen des BIOS Menüs wieder ausgewählt wird. Falls automatische Wahl der Konfiguration aktiviert ist, wird das Netz mit der besten Empfangsqualität ausgewählt. Möchte man sich aber mit einem bestimmten Netz verbinden, so muss dieses als Standard eingestellt sein, und die automatische Konfigurationswahl muss abgestellt werden.



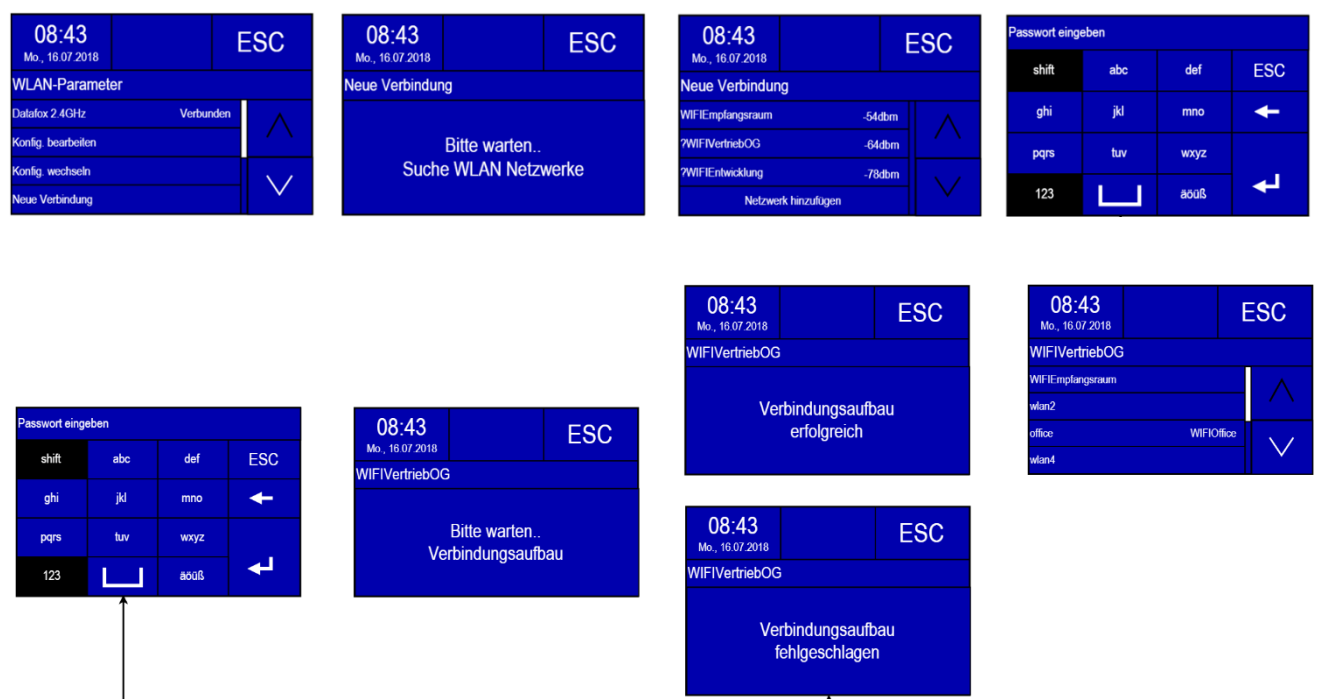
Neue Verbindung

Bei Auswahl von diesem Menüpunkt wird ein Netzwerkscan durchgeführt. Im Anschluss kann aus der Liste der Netzwerke eins ausgewählt werden. Dazu wird dann ein Schlüssel eingetragen (Abbildung 4). Im Anschluss wird versucht eine Verbindung mit dem Netzwerk aufzubauen. Das Ergebnis des Verbindungsaufbaus wird am Bildschirm ausgegeben (Abbildung 5). Konnte eine Verbindung hergestellt werden, so wird im nächsten Dialog ein Speicherplatz ausgewählt. Im Anschluss wird die Konfiguration gespeichert. Falls gewünscht kann die neue Konfiguration direkt als Standard verwendet werden (Abbildung 6). Zusätzlich gibt es noch die Möglichkeit eine Eingabe des SSIDs von Hand vorzunehmen. So können Netzwerke die nicht in Reichweite sind, oder die SSID nicht aussenden hinzugefügt werden.



Achtung:

Aktuell wird bei der Eingabe mit SSID jedoch nur die Verbindung mit WPA2 Netzen unterstützt.



08:43 Mo., 16.07.2018	ESC
WIFIVertriebOG	
WIFIEmpfangsraum	^
wlan2	
office	WIFIOffice
wlan4	v

08:43 Mo., 16.07.2018	ESC
WIFIVertriebOG	
Konfiguration gespeichert	

08:43 Mo., 16.07.2018	ESC
WIFIVertriebOG	
Als Standard verwenden ?	
Ja	Nein

Systeminfo/Erweitert

Im Menüpunkt Systeminfo/Erweitert können Informationen zu der WLAN Hardware erfragt werden. So ist die aktuell erhaltene IP Adresse, die MAC Adresse des WLAN Chips, sowie die eingesetzte Firmware des WLAN Moduls. In Gespeicherte Netze ist die Anzahl der zurzeit genutzten Konfigurationen angegeben. Durch Auswählen des Punktes Konfigurationen zurücksetzen können alle Konfigurationen gelöscht werden. Die Konfigurationen entsprechen dann einem neuen, noch ungefüllten LAN und WLAN Konfiguration. Mehr Informationen zu den aktuellen Kommunikationsparametern finden sich in den Benutzereinstellungen

08:43 Mo., 16.07.2018	ESC
WLAN-Parameter	
Erweitert	^
	v

08:43 Mo., 16.07.2018	ESC
Systeminfo	
IP	192.168.132.32
MAC	00-AA-BB-33-CC-22
Firmware	4.5.5
Gespeicherte Netze	5

08:43 Mo., 16.07.2018	ESC
Systeminfo	
WLAN Konfigurationen löschen	^
	v

Tastatur Eingabe

abfrh			
shift	abc	def	ESC
ghi	jkl	mno	←
pqrs	tuv	wxyz	↵
123	⏏	äöüß	↵

1!=			
1!?:.	2!"><	3\$_-	ESC
4\$*+	5%.,;	6&#	←
7/[µ	8{[-	9]@	↵
abc	0=}\\	latin1	↵

230 æ			
1	2	3	ESC
4	5	6	←
7	8	9	↵
abc	0	123	↵



Hinweis:

Die Eingabe des SSIDs und des Schlüssels sind auf 32 Zeichen begrenzt. Als Eingabe sind Werte des Latin1 Zeichensatzes erlaubt, mit Ausnahme der Steuerzeichen.

5.3.3. Displaydesigner

Anwendungsbereich:

			4.3/4.6	2.8/3.5	5.0	Uni- versal	Agera ZK	Inloc	Mobil Box	IO-Box	Oneloc				EVO- PC
☒	☒	☒	☒	☒	☒	☒	☒								

Bei AE-MasterIV V4, PZE-MasterIV V4 und PZE-MasterIV Basic V4 ist der Designer nur für Farbdisplay anwendbar.

Mit dem Display-Designer bietet Datafox die Möglichkeit für Partner und Anwender die Darstellung den Wünschen entsprechend anzupassen. Aber Achtung aufgrund der notwendigen Bedienfolgen kann das keine komplett freie Gestaltung sein, sondern es müssen schon Dinge wie Kopfzeilen, Menüstrukturen und Fußzeilen gewährleistet sein. Ziel des Display-Designers ist es mit minimalem Aufwand die machbaren Einstellungen zu ermöglichen.

Wir freuen uns auf viele Anwender und empfehlen:

Erstellen Sie sich Ihr firmeneigenes Display-Design:

Beispielbilder für EVO 4.3 und 4.6 FlexKey



Beispielbilder für EVO2.8 / 3.5

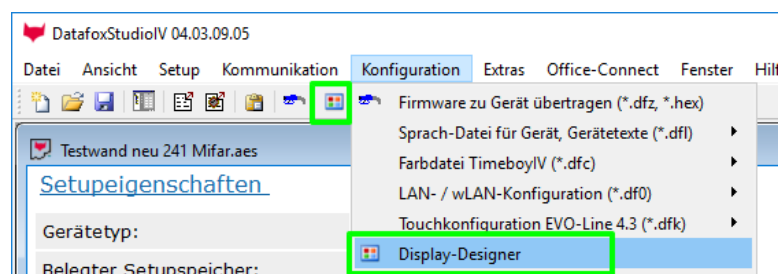


Beispielbilder für PZE-/ AE- Master V4 mit Farbdisplay

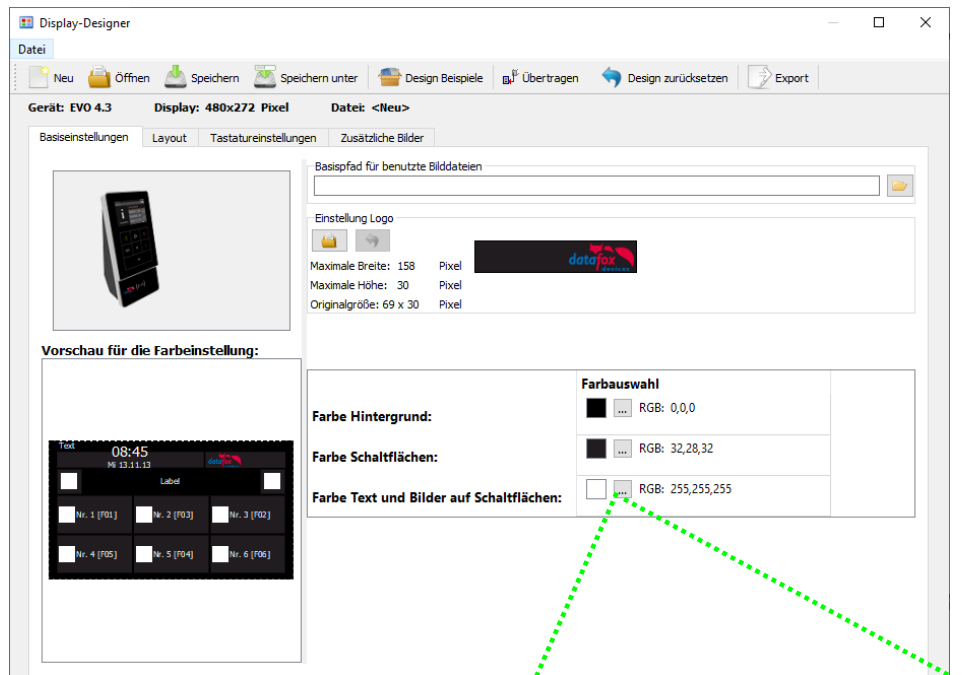


Um für Ihr Gerät eine individuelle Anzeige zu erstellen, benötigen Sie mindestens das DatafoxStudioIV 04.03.09.05.

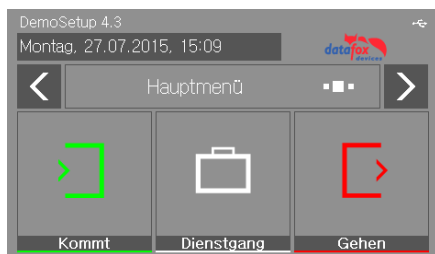
Der Aufruf des Display-Designers erfolgt über das Menü Konfiguration oder direkt aus der Setup-Editier-Maske heraus.



5.3.3.1. Farbeinstellung für die Anzeigen im EVO 4.3 / 4.6 / 2.8 / 3.5 / 5.0



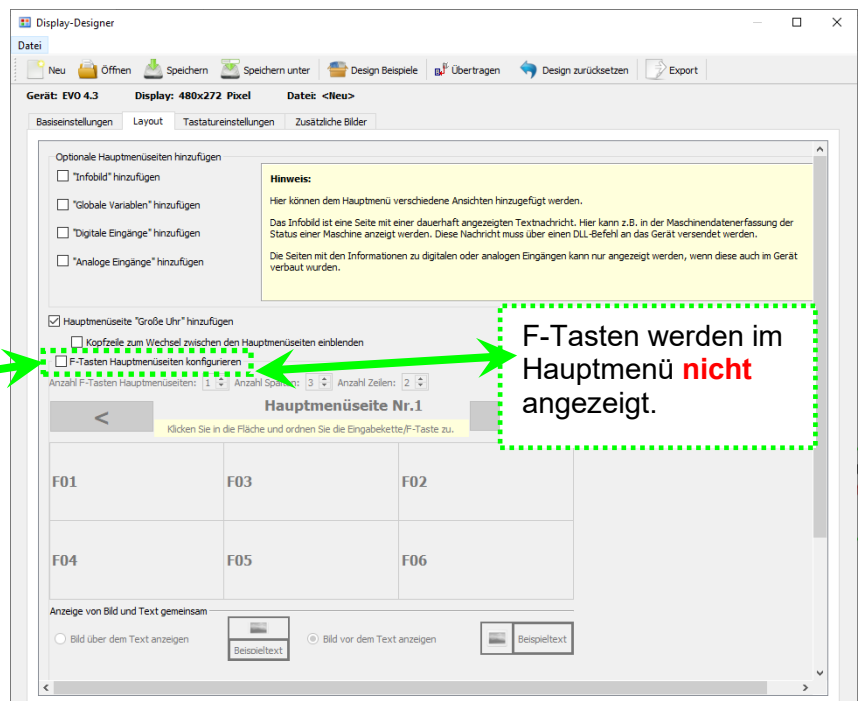
Beispielbild:



5.3.3.2. Standardeinstellungen

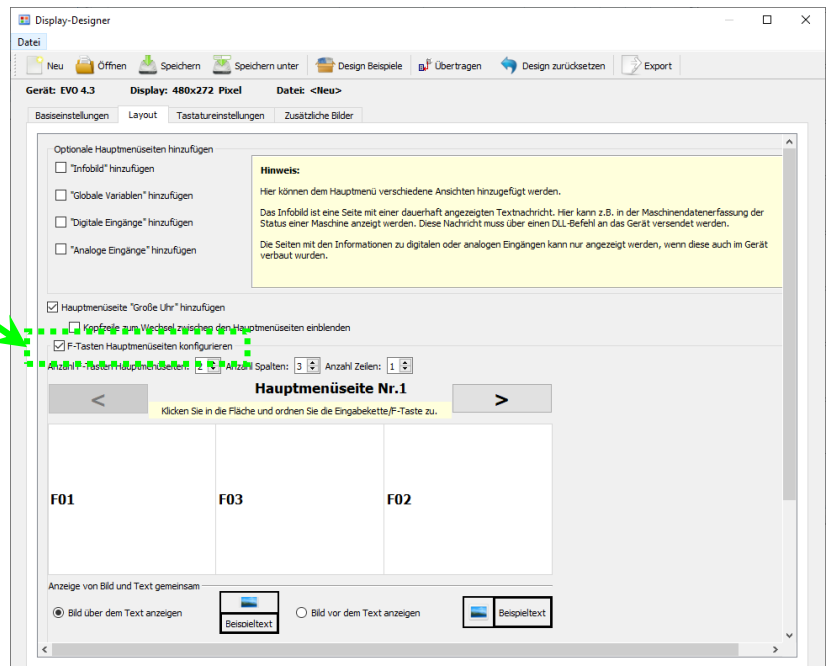
Die Geräte werden im Standard „PZE“ Design ausgeliefert.

Dieses Design ist auch als Standard beim ersten Erstellen eines neuen Designs im Display-Designer voreingestellt.



5.3.3.3. Funktionstasten im Display des EVO 4.3 / 4.6 / 2.8 / 3.5 / 5.0 anzeigen

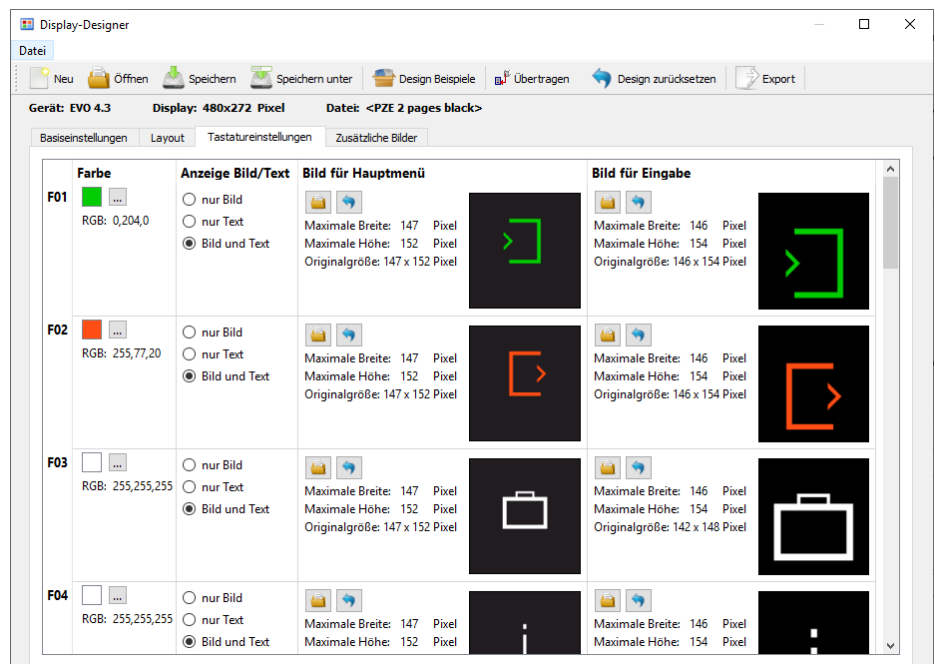
Beispiel:
Durch das Einblenden der Funktionstasten aus dem Setup, kann nun die Anzahl der im Display angezeigten Tasten angepasst werden.



5.3.3.4. Bilder für Funktionstasten des EVO 4.3 / 4.6 / 2.8 / 3.5 / 5.0 hochladen

Unter diesem Menüpunkt „Tasteneinstellungen“ können Sie die Bilddatei für jede Funktionstaste importieren.

Beispielbild für die Tastenbilder:



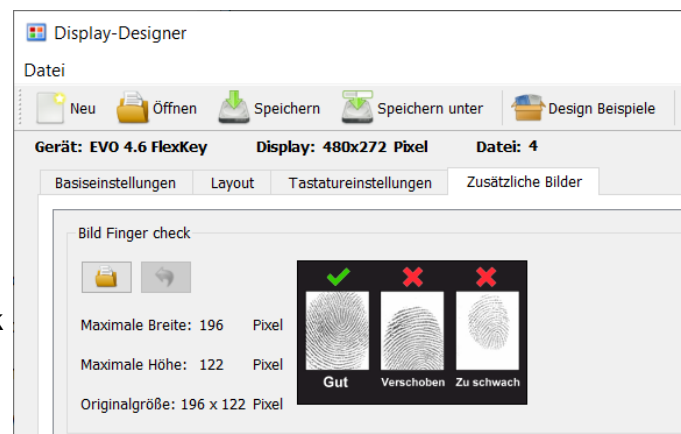
5.3.3.5. Zusätzliche Bilder übertragen

Es können auch zusätzliche Bilder auf dem Terminal hinterlegt werden. Diese können entweder bei der Datenspeicherung, in Eingabefeldern, als Tastaturlayout oder im Fingerprintmenü dargestellt werden. Auf diese Weise kann Ihr Terminal noch besser auf Ihre Anforderungen und Anwendungsgebiete angepasst und individualisiert werden.

5.3.3.6. Bild für das Fingerprintmenü hochladen

Bei Terminals mit einem Fingerprint Flächensensor gibt es zum Einlernen, Trainieren und Löschen der Fingerprinttemplates ein separates Menü. Im Menüpunkt „Prüfen“ kann man sein Finger auf den Sensor legen und ein Bild des Fingerabdruckes wird angezeigt. Somit kann man die Position des Fingers auf dem Sensor und den Auflagedruck überprüfen.

Um die korrekte Position und den richtigen Druck noch einmal zu verdeutlichen, kann man ein Bild zum Vergleich anzeigen. Dieses kann hier ausgewählt werden, sollte es vom Standard abweichen.



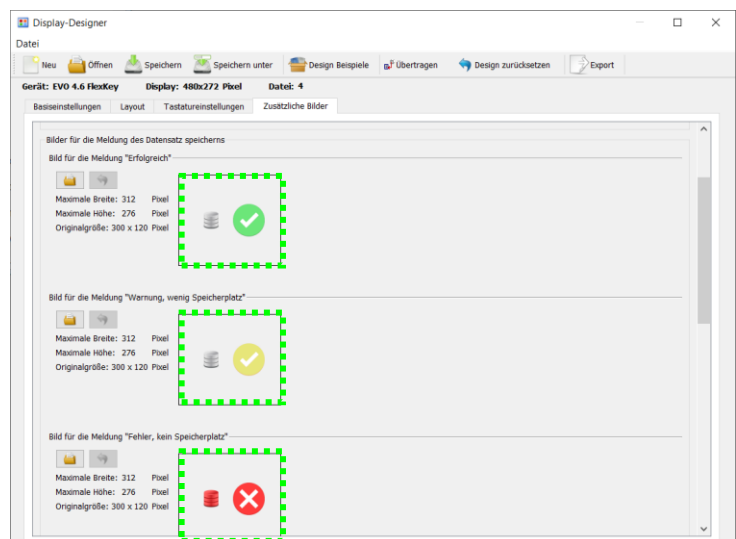
5.3.3.7. Bilder für die Datenspeicherung hinterlegen

Die drei Bestätigungsmeldungen nach Abschluss und Speicherung eines Datensatzes können nun mit einer Grafik dargestellt werden.

Die zu sehenden Grafiken sind im Standard hinterlegt und werden anstatt der Meldungen am Display des Terminals angezeigt.

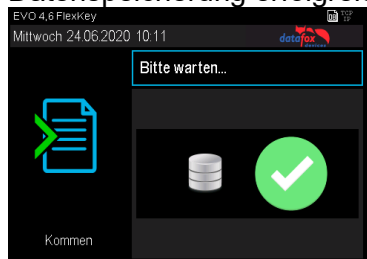
Wenn Sie eigene Bilder für diese Meldungen einstellen möchten, müssen diese einmalig übertragen werden.

Bei den Dateibezeichnungen müssen folgende Namensgebungen eingehalten werden:

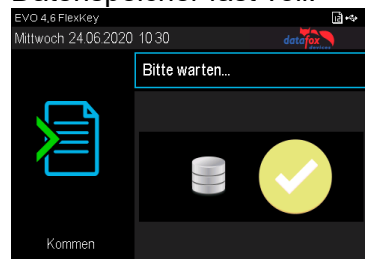


Dateiname für erfolgreiche Datenspeicherung: *save_ok.bmp*
 Dateiname für Warnung bei fast vollem Speicher: *save_warning.bmp*
 Dateiname für Fehler bei vollem Speicher: *save_error.bmp*

Datenspeicherung erfolgreich!



Datenspeicher fast voll!



Datenspeicher voll! Admin benachrichtigen!



Hinweis:

Die Grafiken müssen nicht gesondert aktiviert werden, d.h. es genügt sie zum Gerät zu übertragen. Sobald eine der Grafiken vorliegt, wird sie immer anstatt des Textes dargestellt.

Diese Option ist für alle Terminals mit Farbdisplay verfügbar:

✘	✘	✘	✘	✘	✘	✘	✘	✘							

Bild im Hauptmenü anzeigen

Im Hauptmenü des Terminals kann nun eine Grafik, anstatt der „großen Uhr“, globalen Variablen, etc., angezeigt werden. Diese kann Informationen, wie zum Beispiel den Termin für die nächste Firmenfeier oder den aktuellen Essensplan der Kantine, beinhalten.

Dateiname: *main.bmp*

Bild für das Hauptmenü

Maximale Breite: 472 Pixel
 Maximale Höhe: 276 Pixel
 Originalgröße: 276 x 276 Pixel



Hinweis:

Zum Aktivieren der Grafik genügt es, sie zum Gerät zu übertragen. D.h. sowie sie im Gerät vorliegt, wird sie beim Wechsel ins Hauptmenü bevorzugt angezeigt. Nach wie vor sind durch Wischen die anderen, im Display-Designer aktivierten Hauptmenüseiten zu erreichen.

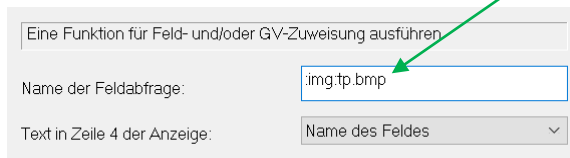
5.3.3.8. Tastaturgrafik und Touchkonfiguration des EVO 4.6 FlexKey und EVO 5.0

! Nur ein Kapitel für EVO 5.0 und EVO 4.6

5.3.3.9. Bilder in Eingabefeldern anzeigen

In den Eingabefeldern „Normal“, „Fingerprint“, „Bestätigung“ und „Nachricht anzeigen bzw. warten“ ist es möglich statt eines Textes oder der großen Uhr ein Bild darzustellen.

Der Name des Eingabefeldes definiert, welches hinterlegte Bild angezeigt wird. Der Bildname muss in folgender Form im Namen der Feldabfrage eingetragen werden. „:img:bild.bmp“



Eine Funktion für Feld- und/oder GV-Zuweisung ausführen

Name der Feldabfrage:

Text in Zeile 4 der Anzeige:

Dabei ist der Teil *bild.bmp* durch den eigentlichen Bildnamen zu ersetzen, hier am Beispiel „*tp.bmp*“.



Achtung:

Da für den Namen der Feldabfrage maximal 16 Zeichen eingegeben werden können und das Label für ein Bild mit „:img:“ beginnen muss, darf der eigentliche Bildnamen aus noch höchstens elf Zeichen bestehen.



Achtung:

Diese Funktion steht bei den PZE- und AE-MasterIV-Geräten nur in Verbindung mit einem Farbdisplay zur Verfügung. Für EVO 2.8 Pure, EVO 3.5 Pure und EVO 3.5 Universal ist dieses Feature nicht möglich, da sonst die F-Tasten zur Bedienung nicht mehr dargestellt werden könnten.

Beispielbilder Feldfunktion „Normal“ & „Nachricht anzeigen bzw. warten“:

EVO 4,6 FlexKey
Mittwoch 24.06.2020 11:07

Kommen

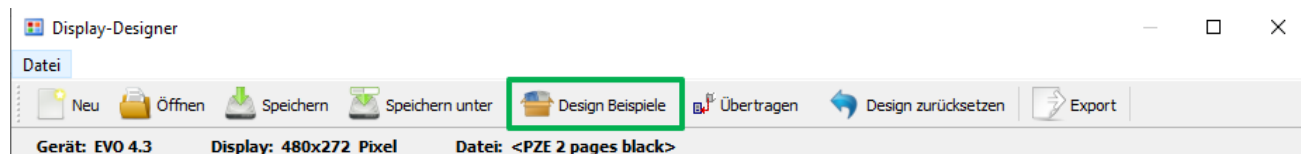
EVO 4,6 FlexKey
Mittwoch 24.06.2020 11:07

Kommen

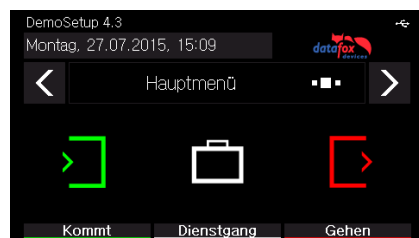
Die Anzahl der zu ladenden Bilder kann individuell eingestellt werden. Alle Bilder, die hier verknüpft sind, werden auch auf das Terminal übertragen. Sind diese nicht in einem Eingabefeld verwiesen, werden die Bilder auch nicht angezeigt. Beachten Sie in diesem Fall, dass der verfügbare Speicherplatz im Terminal dadurch verringert wird.

5.3.3.10. Designbeispiele im Designer enthalten

Mit der Installation des DatafoxStudioIV erhalten Sie verschiedene Designbeispiele für die Geräte. Über den Button „**Design Beispiele**“ lassen sich diese öffnen.

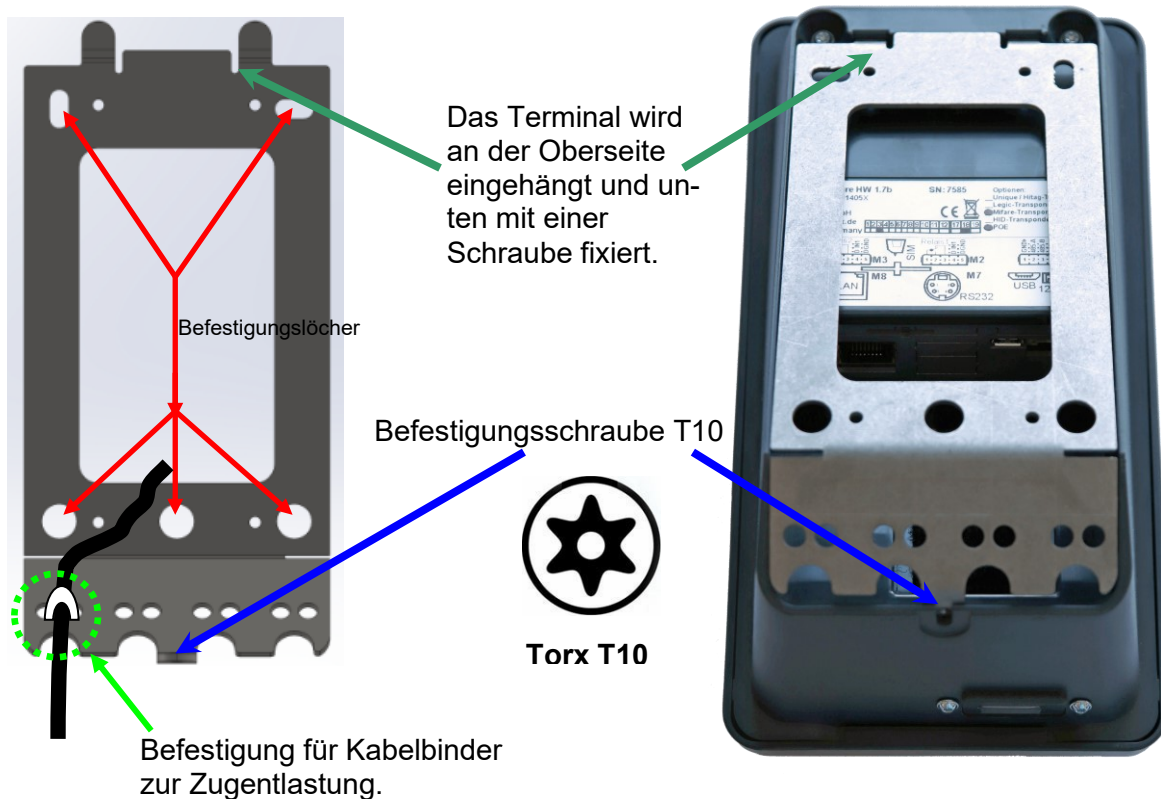


Die Beispiele werden von Datafox nach und nach erweitert. Sollten Sie hierzu Anregungen und Wünsche haben, dann teilen Sie uns diese gerne mit.



5.4. Montage des EVO2.8/3.5/5.0 Pure Terminal

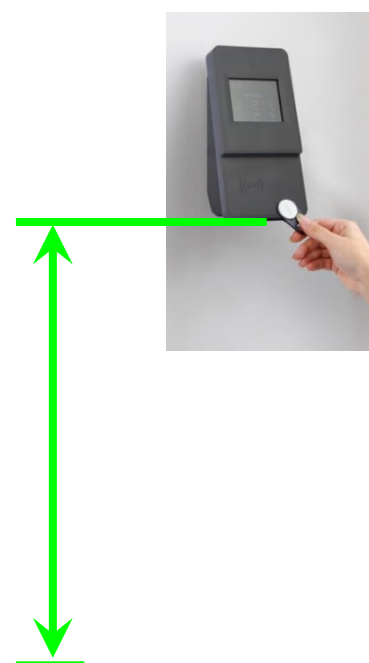
Die Wandmontage erfolgt mittels einer Wandhalterung. Diese wird über 4 Befestigungspunkte an der Wand befestigt.



5.4.1. Montagehöhe des EVO 2.8/3.5/5.0

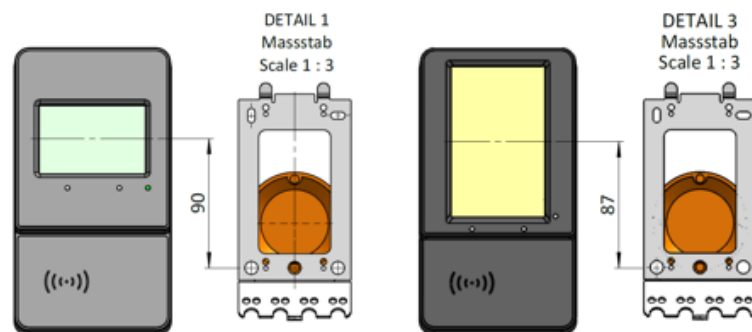
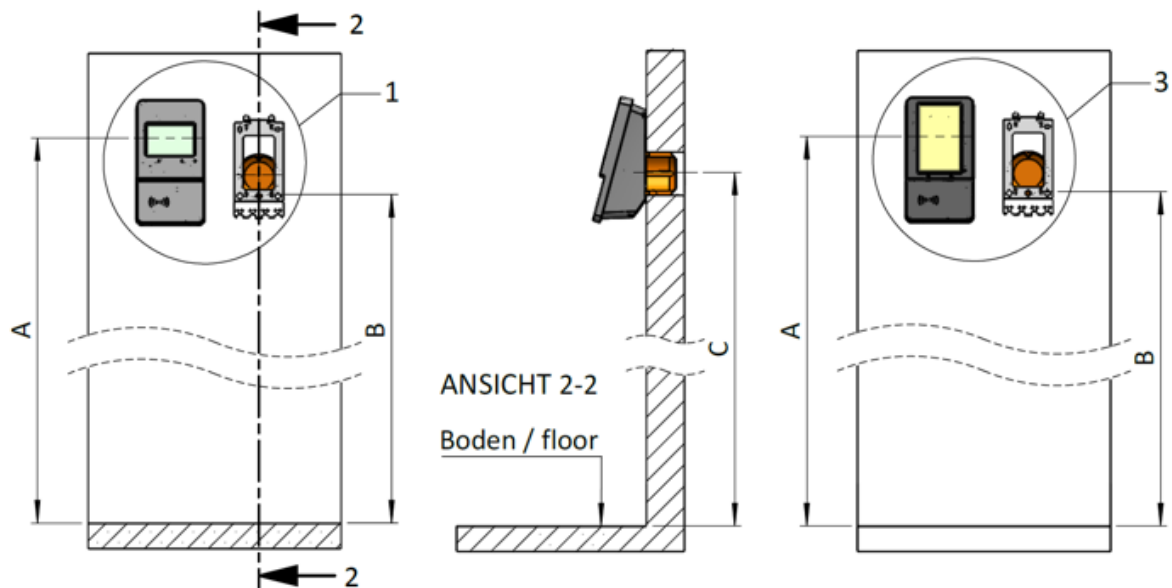
Je nach Personengröße wird eine Installationshöhe von 1,20 bis 1,40 m empfohlen.

Wenn das Gerät mit Fingerscanner ausgestattet ist, sollten Sie das Gerät 5 cm bis 10 cm höher anbringen.



5.4.2. Alle Maßangaben für das EVO 2.8/3.5/5.0 Terminal

Montage / installation



		EVO 3.5 / 5.0 Pure ohne / without FP	EVO 3.5 / 5.0 Pure mit / with FP
A	empfohlene Einbauhöhe <i>recommended installation height</i>	1350mm	1250mm
B	Höhe Montagebohrung Wandhalterung <i>Height of mounting hole Wall bracket</i>	1230mm	1130mm
C	empfohlene Höhe Kabelausgang / UP-Dose <i>recommended height cable outlet / flush-mounted box</i>	1260mm	1160mm

Die passende Bohrschablone finden Sie hier:

https://www.datafox.de/downloads-evo-line-28.de.html?file=files/Datafox_Devices/Downloads_Module_Zubehoer/230_Montage/114051%20EVO%203.5%20Pure%20Bohrschablone.pdf

Tischständer:

https://www.datafox.de/downloads-evo-line-43.de.html?file=files/Datafox_Devices/Downloads_Module_Zubehoer/230_Montage/11x081%20EVO%20Tischstaender%20BG%20%2B%20Geraete.pdf

Blatt für die Montagezeichnung für alle Geräte:

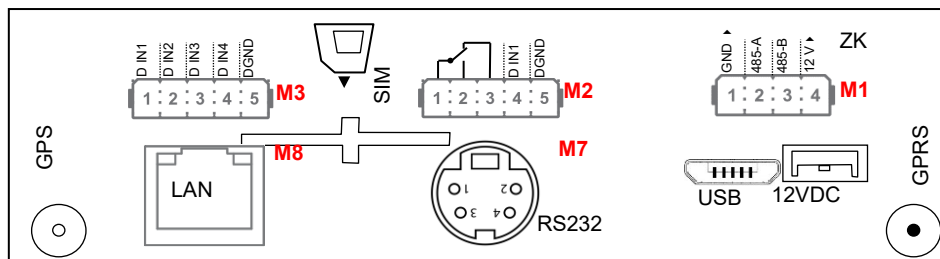
https://www.datafox.de/downloads-evo-line-28.de.html?file=files/Datafox_Devices/Downloads_Module_Zubehoer/230_Montage/Datafox%20EVO%203.5%20Pure%20-%20EVO%204.3%20Montagezeichnung.pdf

5.5. Anschluss des EVO2.8 /3.5/5.0/ Pure Terminals

5.5.1. Steckerbelegung

Das EVO 2.8 Pure Terminal verfügt über 5 Modulplätze.

Standardbestückung siehe Anschlussbild (nur mit optionaler Bestellung der einzelnen Module):



Steckerleiste des EVO 2.8 Pure V4

Bezeichnung	Modul	PIN	Beschreibung
Modulplatz 1	1	1	GND
		2	A RS 485 für Zutrittskontrolle
		3	B RS 485 für Zutrittskontrolle
		4	12 V
Modulplatz 2	2	4-5	Standard: 1 digitaler Eingang
		1-3	1 digitaler Ausgang mit Wechsler -Kontakt
Modulplatz 3	3	1	1 digitaler Eingang
		2	2 digitaler Eingang
		3	3 digitaler Eingang
		4	4 digitaler Eingang
		5	GND
Modulplatz 7 RS 232 Mini-DIN M004	7	1	TXD
		2	RXD
		3	+ 5 V
		4	Ground / GND
Modulplatz 8	8		TCP/IP - LAN RJ 45

5.5.2. Spannungsversorgung des EVO 2.8 / 3.5 / 5.0 / Pure

Die Versorgungsspannung geschieht mittels eines Netzteils 12V DC / 18 W.

Das Terminal selbst kann mit einer Versorgungsspannung von 24 V DC versorgt werden.

Achtung! Bei der Verwendung der ZK-Erweiterung wird die Versorgungsspannung direkt für die ZK-Module weiter gereicht. Diese darf dann 12 V nicht überschreiten.

Das Netzteil:



5.6. Spannungsversorgung über POE

Optional können die Geräte mit einem POE-Modul (Art. Nr.: 114117) ausgestattet werden. Es gibt 2 Standards die bei der EVO-Line unterstützt werden.

PoE-Standard		Leistung pro Port	nutzbare Leistung
PoE	IEEE 802.3af	15,4 Watt	12,95 Watt
PoE+	IEEE 802.3at	25,4 Watt	21,90 Watt

Erfolgt die Spannungsversorgung über POE, kann bei angeschlossener Zutrittskontrolle auch ein Externer Leser über den Anschluss der ZK mit versorgt werden.

5.6.1. Wichtige Hinweise für die Nutzung von POE

Auf was ist zu achten?

Als erstes müssen Sie feststellen, welche Hardwaregeneration Sie über POE betreiben möchten. Hardware V4, V3, V2 oder V1. Wie Sie das feststellen, finden Sie hier: [Link](#)

Hardware V4:

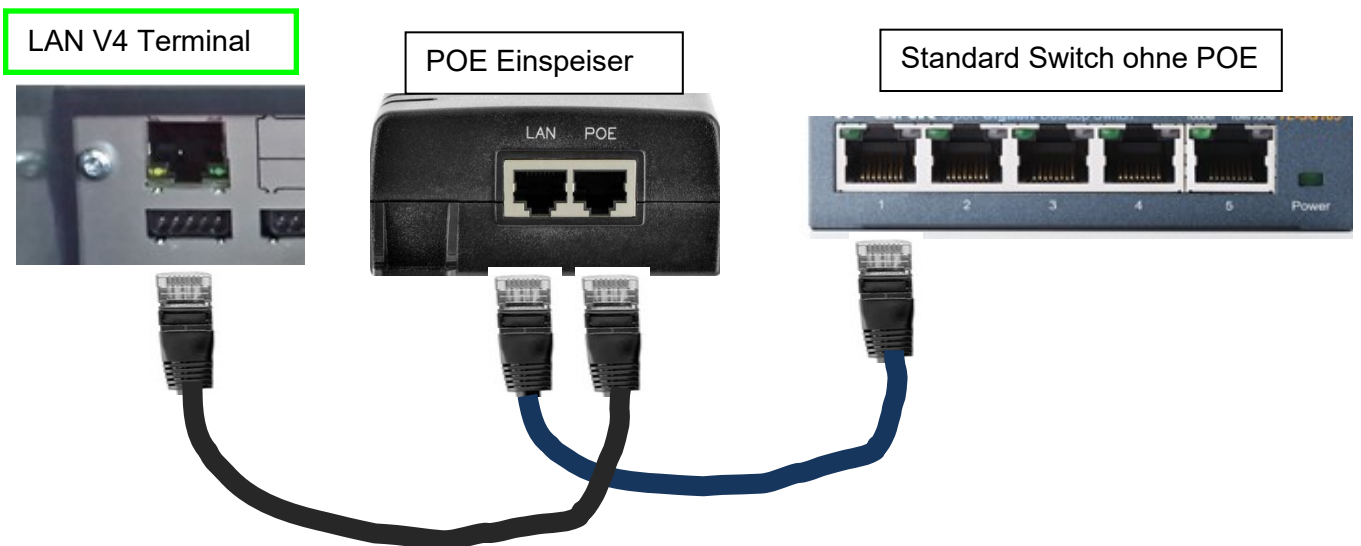
Bei der Hardware V4 kann optional POE bestellt werden. Unabhängig davon, ob diese Option bestückt ist, können Sie die Geräte direkt an ein POE Netzwerk anschließen.

Dabei spielt es keine Rolle, ob die Einspeisung über den Switch direkt erfolgt oder über einen POE-Einspeiser.

Variante 1: „Einspeisung POE“ direkt über den POE-Switch:



Variante 2: „Einspeisung POE“ über einen separaten Einspeiser:



Hardware V3, V2 oder V1:

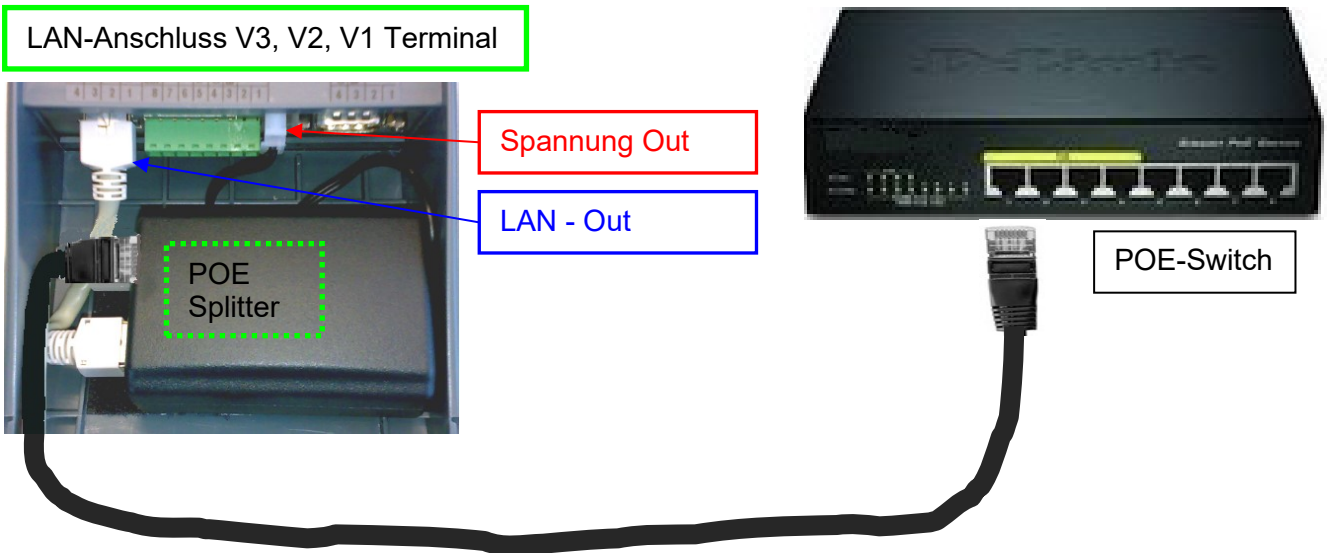
Bei dieser Hardware kommt ein Lantronix XPort für die Kommunikation im IP-Netzwerk zum Einsatz. Bei diesem Produkt darf laut Herstellerangabe auf keinen Fall die POE-Spannung direkt angelegt werden, sondern nur über einen POE-Splitter mit POE betrieben werden.



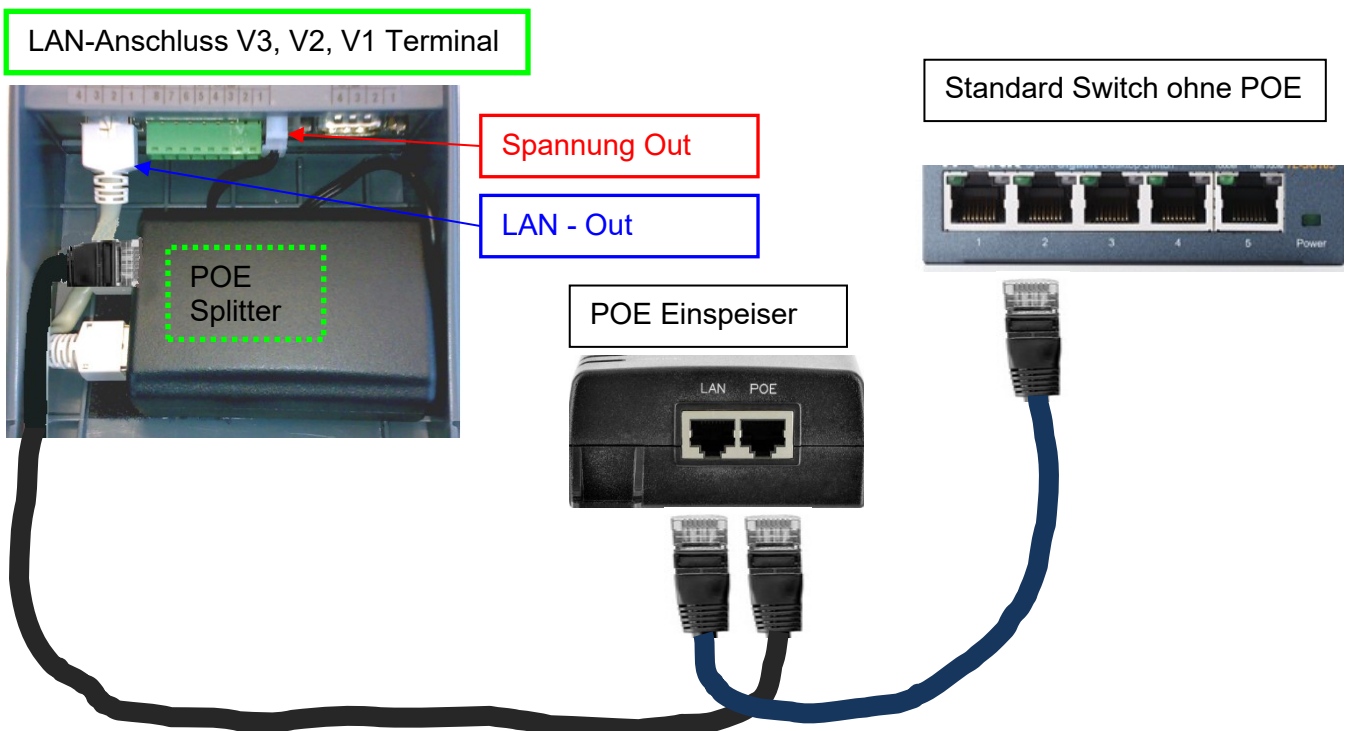
Achtung:

Sie dürfen das Netzkabel mit POE nicht direkt an die LAN Buchse anschließen. Dies kann zur Zerstörung des LAN Anschlusses (XPort) führen. Der XPort ist nicht POE kompatibel.

Variante 1: „Einspeisung POE“ über den POE-Switch und angeschlossenen Splitter:



Variante 2: „Einspeisung POE“ über einen separaten Einspeiser:



Welche Hardware habe ich vorliegen?

Möglichkeit 1:



Schauen Sie auf das Typenschild. Dies finden Sie auf der Rückseite des Gerätes.
Hier ein Beispiel für einen PZE-MasterIV **V3**.

Möglichkeit 2:

Am Gerät selbst, haben Sie die Möglichkeit im BIOS-Menü sich über die Firmware des Gerätes zu informieren. Diese gibt aufgrund Ihrer Kennung „04.XX.XX“ genaue Auskunft, um welche Hardware es sich handelt.

Hardware **V4** = Firmware 04.03.XX

Hardware **V3** = Firmware 04.02.XX

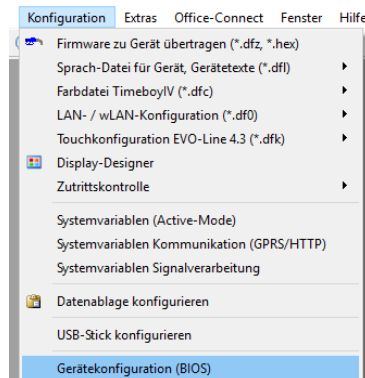
Hardware **V2** = Firmware 04.01.XX

Hardware **V1** = Firmware 04.01.XX

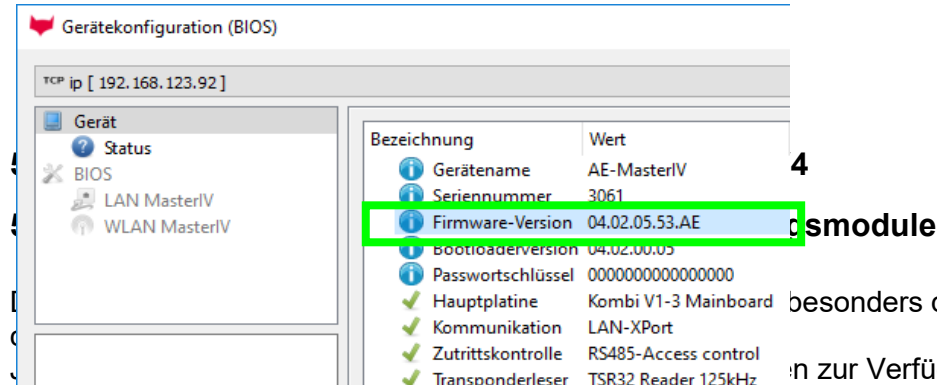
Wie Sie das Biosmenü öffnen, finden Sie Kapitel „Aufbau BIOS-Menü“.

Möglichkeit 3:

Lesen Sie mit dem aktuellsten DatafoxStudioIV die Firmwareversion aus:








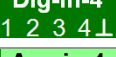
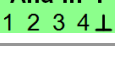
Klicken Sie auf:
„Konfiguration“
->
„Gerätekonfiguration (BIOS)“
dann auf „Lesen“



Diese können nun individuell mit den einzelnen zur Verfügung stehenden Modulen bestückt werden.

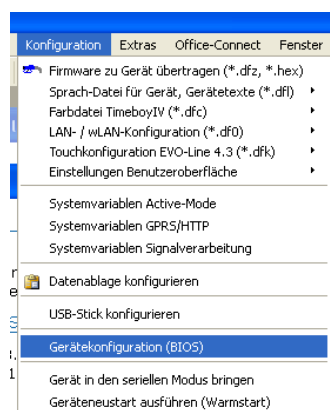
Abhängig von der Größe des Moduls belegen die einzelnen Module ein oder zwei Modulplätze. So benötigt z.B. das GPRS (Mobilfunk) 2 Modulplätze und ein Relais-Modul nur einen Modulplatz.

Übersicht über die Modulbaugruppen:

Modul Bezeichnung	benötigte Modulplätze	Beschreibung im Bios Modul_Nr.:	Max. mögliche Anzahl des Moduls	Artikel Nr. für den Stecker	Aufdruck & Farbe
RS 232 - mini DIN Barcode	1	032 Serial Port mini DIN 5V max. 500 mA	1		
RS 485 Zutritt	1	014 RS485 + 12V Supply Max. 500 mA	3 Displaygeräte 4 KYO-Inloc	A3100004-01	
RS 485 Hauptkommunikation	1	035 RS 485 Com Port	1	A3100004-01	
GPRS Mobilfunk	2	Mobile MC 55i	1		
TCP/ IP	1	011 Ethernet Port	1		
WLAN	1	001 WLAN Red Pine	1		
2x digital Out	1	005 Digitalausgang Relais	8	A3100005-01	
4x digital Out	1	051 Digital Ausgang aktiv GND	8	A3100005-08	
4x digital Out	1	051 Digital Ausgang aktiv positiv (Plus)	8	A3100005-05	
1x digital In + 1x digital Out	1	012 Digital In-/Output	8	A3100005-04	
4x digital In	1	006 Digital Input	8	A3100005-02	
4x analog In	1	008 Analog Input	8	A3100005-03	

Wie viele Modulplätze in dem jeweiligen Datafox Gerät zur Verfügung stehen, finden Sie im Gerätehandbuch unter dem Kapitel „Geräte-Anschluss“.

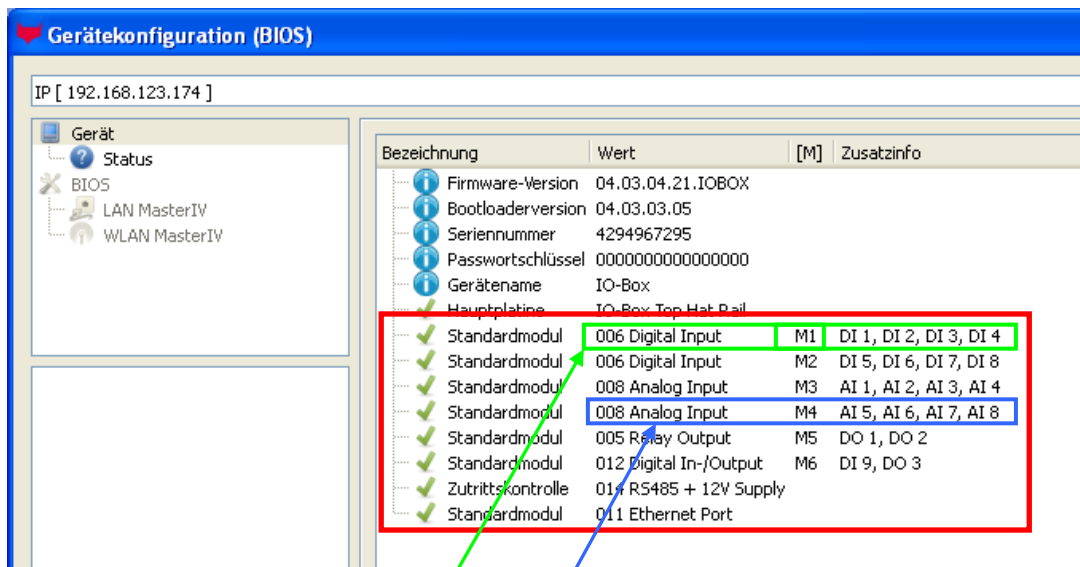
5.7.2. Bestückung von Modulen aus Gerät lesen



Klicken Sie auf:
„Konfiguration → Gerätekonfiguration Bios“
dann
klicken Sie auf „Lesen“.

Anzeige im Bios:

Hier werden Ihnen alle Module angezeigt, die im Gerät eingebaut sind. Gleichzeitig erhalten Sie die Information, an welchem Modulplatz was bestückt ist und wo sich welcher Ein- Ausgang befindet.



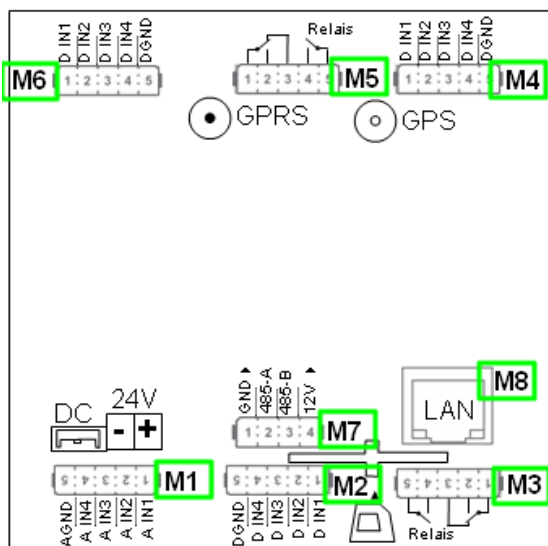
Beispiel 1:

- Modulplatz = M1
- digitaler Eingang 1 bis 4
- Modul_Nr.: = 006

Beispiel 2:

- Modulplatz = M4
- analoger Eingang 5 bis 8 (für das Setup)
- Modul_Nr.: = 008 Analog Input

Beispiel Typenschild einer IO-Box V4:

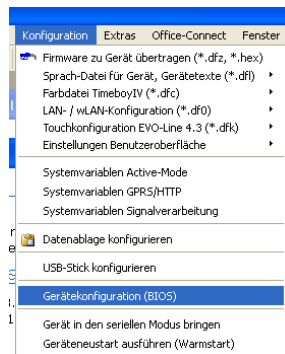


Hier sehen Sie, dass die IO.Box V4 über **8** Modulplätze verfügt. Diese können nun individuell bestückt werden.

Ausnahmen:

- Modulplatz 8, nur an diesem geht TCP/IP
- Wird auf TCP/IP verzichtet, kann hier auch ein anderes Modul bestückt werden.
- RS 485 für Zutritt können max. 4 Module bestückt werden.

5.7.3. Wichtige Modulinformationen vom Gerät auslesen



Klicken Sie auf:
 „Konfiguration → Gerätekonfiguration Bios“
 dann auf „Status“ danach
 klicken Sie auf „Lesen“.

Device configuration (BIOS)

* Com_3_fest [COM3]

Device

- Status
- BIOS
- LAN MasterIV
- WLAN MasterIV

```

[SETUP]
Status=Running
Name=IO_BOX_AIN_DigIN_2xRel.aes
1 Time=2017-01-30 09:17:44
2
3 [IN]
4 Status=00000000-
5
6 [CNT]
7 Values=-
8
9 [OUT]
10 Status=000
11
12 [ANALOG]
13 Values=0.01 V, 0.01 V, 0.01 V, 0.01 V, 0.01 V
14
15 [TIMER]
16 Time to next trigger 1 (2)
17
18 [MEMORY]
19 Size=4194304
20
21 [RECORDS]
22 Size=786432
23 Free=785980 (99%)
24 Used=452 (1%)
25 Count=4
26
27 [LAN]
28 Mac=E4-F7-A1-00-0B-5E
29 Ip=192.168.1.122
30 Mask=255.255.255.0
31 Gateway=0.0.0.0
          
```


Hier werden Ihnen eine ganze Reihe wichtiger Informationen zum Terminal ausgegeben.
Hier einige Erläuterungen zu den einzelnen Zeilen:

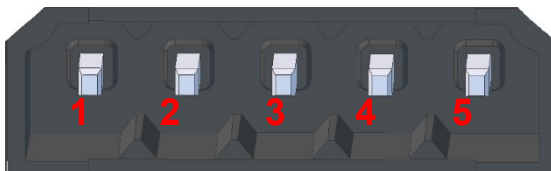
- 1) Name des Setup, diesen erhalten Sie auch beim Auslesen wieder.
- 2) Datum, an dem das Setup in das Gerät eingespielt wurde.
- 3) Zustand der digitalen Eingänge. Alle Eingänge die physikalisch vorhanden sind und im Setup definiert sind, werden hier mit den Zustand angezeigt.
 - a. 00000000 = Im Setup definierte digitale Eingänge
 - b. 0 = Eingang auf low (logisch 0)
 - c. 1 = Eingang auf hi (logisch 1)
- 4) Sind im Setup Zähler über digitale Eingänge definiert, so wird hier der aktuelle Zählwert angezeigt
- 5) Zustand der digitalen Ausgänge: Ausgang 1 ist hier links nach rechts fortlaufend.
- 6) Analogeingänge von links nach rechts mit jeweilig aktuell anliegender Spannung.
- 7) Zustand / Laufzeit von verwendeten Timern
- 8) Anzahl der gespeicherten Datensätze im Gerät und belegter Speicher.

5.7.4. Anschluss der einzelnen Modulbaugruppen

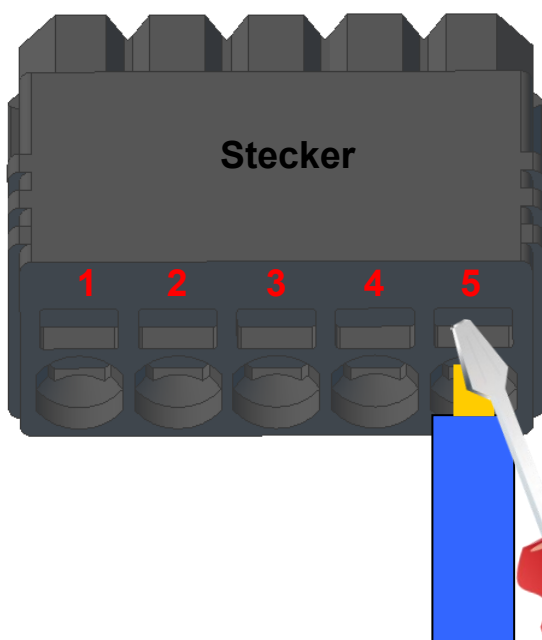
In den nachfolgenden Bildern wird der Stecker für die verschiedenen Anschlüsse in schwarz dargestellt. Die mitgelieferten Stecker sind mit Beschriftung und weiß.

Der Anschlussstecker / Buchse für die Modulbaugruppe hat immer folgende Belegung:

Buchse am Gerät



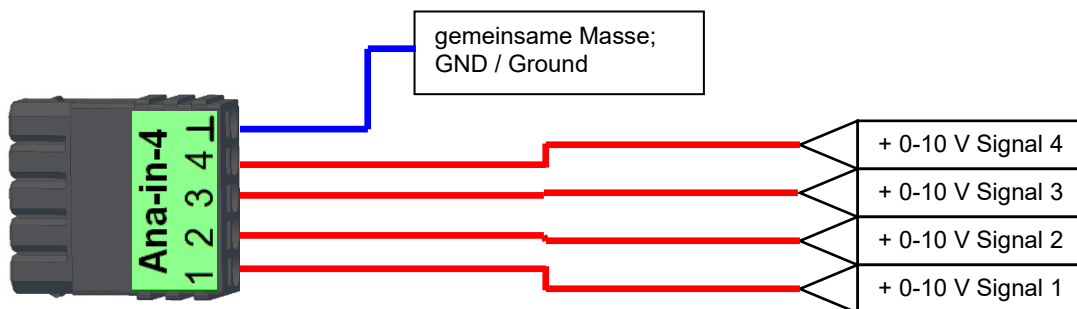
Der Stecker kann nur in einer Richtung eingesteckt werden und ist somit verpolungssicher.



An diesem Stecker können folgende Querschnitte angeschlossen werden:
Massive Drähte = 0,8mm²
Flexible Drähte = 0,6mm²

Zum Lösen der Leitung nutzen Sie bitte einen kleinen Schraubendreher. Massive Drähte können durch leichtes hin- und herdrehen am Draht und Stecker gelöst werden.

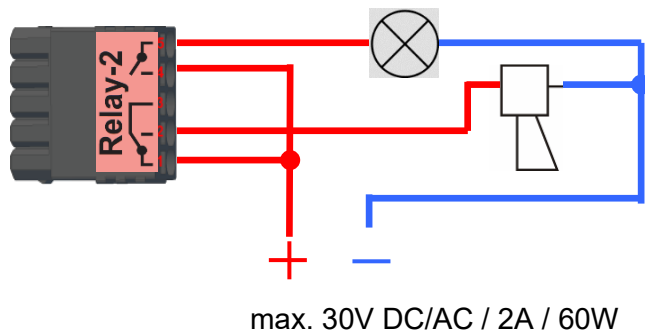
5.7.4.1. Analogeingänge, 4 mal analog IN



5.7.4.2. 2 mal digital Out

Anschlussbeispiel:

(Anschluss einer Signalleuchte und einer Signalleuchte über einen potentialfreien Kontakt):



5.7.4.3. 1 mal digital Out 1x digital IN

Anschlussbeispiel (Anschluss einer Signalleuchte und eines Türkontakts):

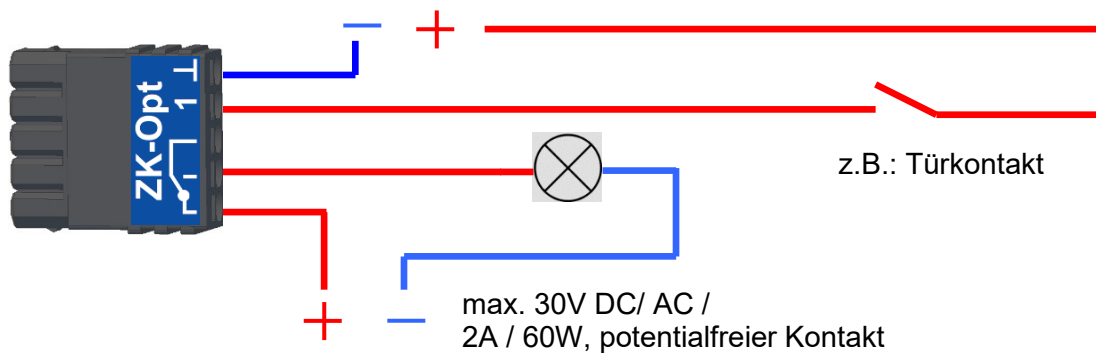
max. 30V

0 - 1,5 V Eingang logisch 0

3,5 V - 30 V Eingang logisch 1

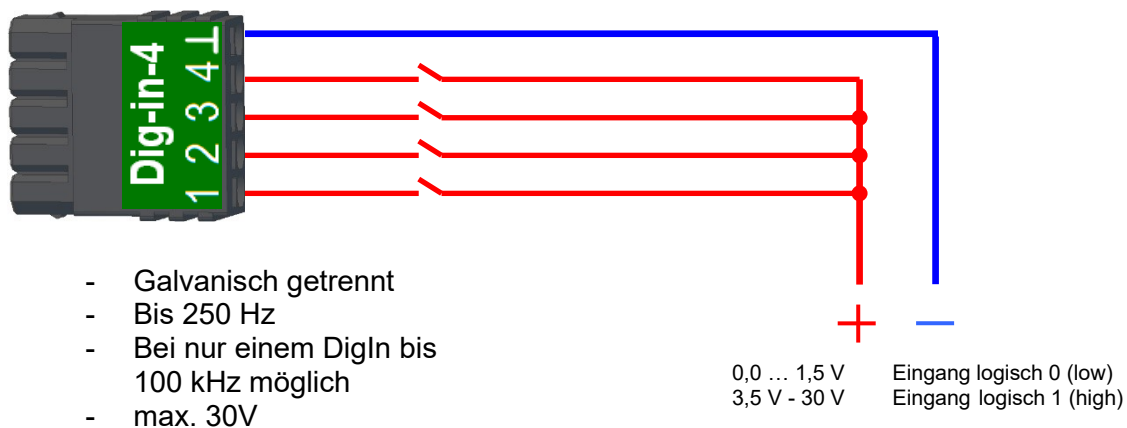
- Galvanisch getrennt

- bis 250 Hz



5.7.4.4. 4 mal digital IN

Anschlussbeispiel (Anschluss von 4 Kontakten):

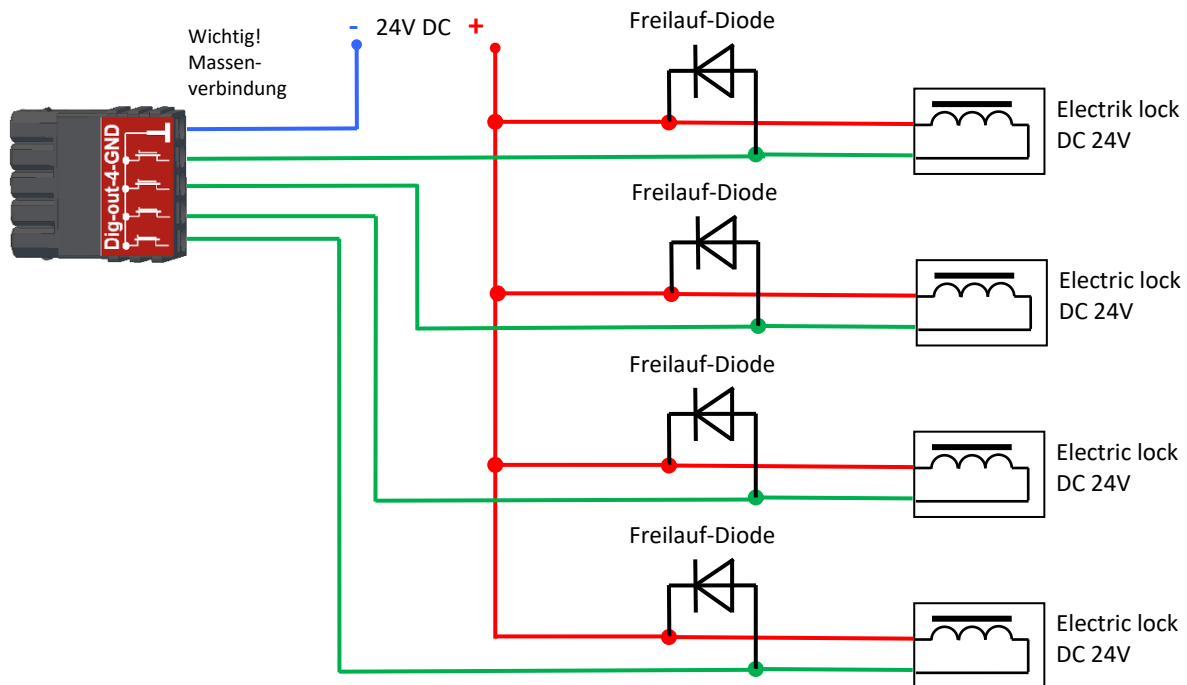


- Galvanisch getrennt
- Bis 250 Hz
- Bei nur einem DigIn bis 100 kHz möglich
- max. 30V

5.7.4.5. 4 mal digital OUT aktiv-Low (Masse geschaltet)

Die digitalen Ausgangsmodule stellen 4 Schaltausgänge auf einem einzigen Modul bereit. Das Modul 51 (Art.-Nr. xxx 172) kann aktiv 12 V DC an jedem Ausgang ausgeben, das Modul 105 (Art.-Nr. xxx 173) schaltet die Ausgänge gegen Masse (Open Drain).

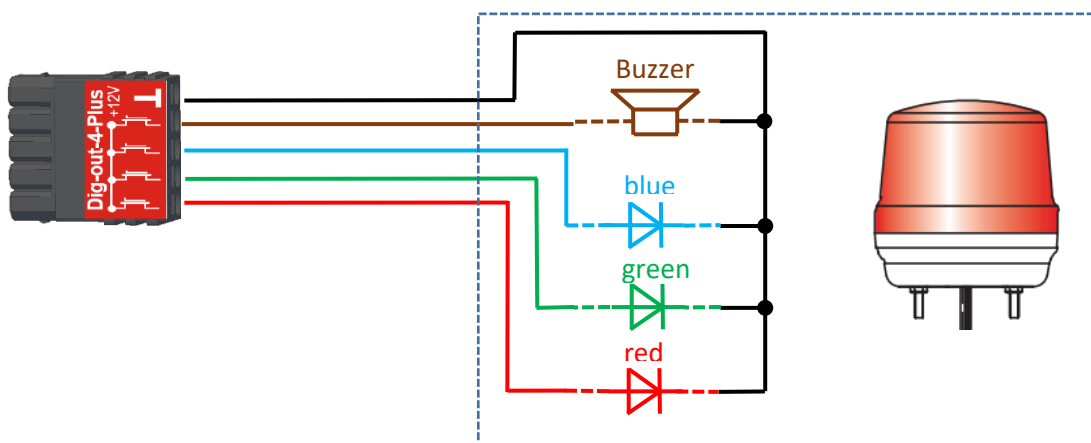
Durch das Schalten gegen Masse, kann das Modul 105 recht große Ströme schalten, z.B. für Schließfächer oder elektrische Türöffner.



5.7.4.6. 4 mal digital OUT aktiv-Hi (Plus geschaltet)

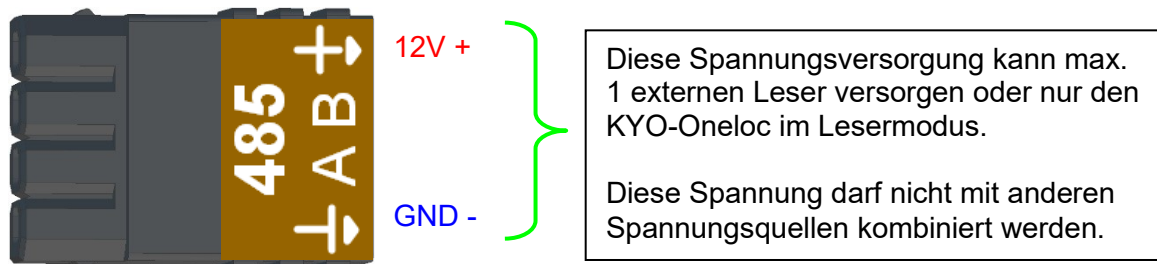
Beispiel Anschluss Meldelampe, Modul 51

Die Störungs-Meldelampe kann auf diese Weise mit nur einem einzigen Stecker angeschlossen werden.



5.7.4.7. RS-485 Bus für ZK

Mit der Option Zutrittskontrolle ist der Anschluss für Externe Leser am Gerät vorhanden.
Die Belegung des Steckers sieht wie folgt aus:



Hinweis:

Die **12 V** liegen sofort nach einschalten der KYO-Inloc an.
Die Zutrittskontrolle wird aber erst aktiv, wenn die Zutrittslisten übertragen wurden.

Weiterhin ist der Anschluss für einen digitalen Ein- und Ausgang vorhanden.
Die Belegung des Steckers sieht wie folgt aus:



Wie die einzelnen Zutrittskomponenten angeschlossen bzw. verdrahtet werden, finden Sie im Kapitel [„Zutrittskontrolle“](#)

5.8. 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:

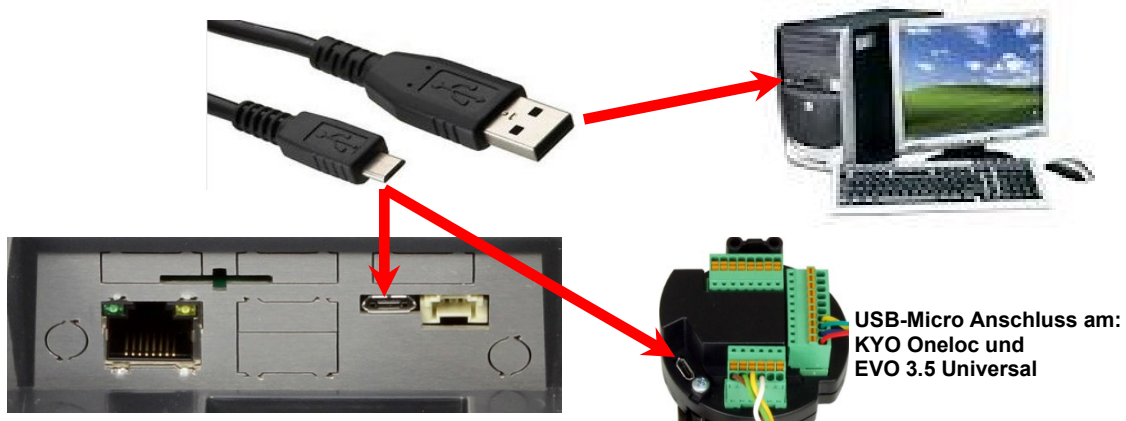
1. über Systemmenü Bios am Gerät
2. ab Firmware 04.02.04 im Setup mit der Feldfunktion „Kommunikation umschalten“. Mehr hierzu finden Sie im Handbuch [DatafoxStudioIV](#).

Mögliche Kommunikationsarten sind:

1. USB (an PC)
2. USB Host, Daten auf USB-Stick speichern
3. TCP/IP über LAN
4. TCP/IP über das Internet (per HTTP)
 - a. Level 0
 - b. Level 1 mehr dazu in der Doku „[Datafox SDK Kommunikation HTTP\(S\)](#)“
5. TCP/IP über WLAN
6. GPRS Verbindung über das Mobilfunknetz

5.8.1. 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.



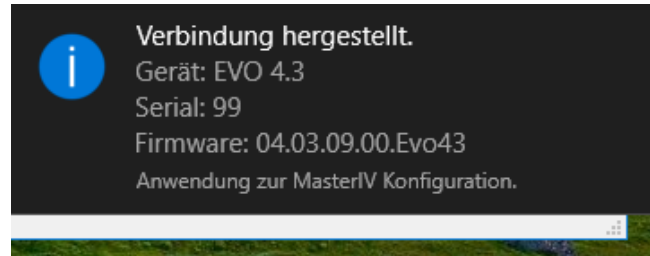
Achtung:

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.

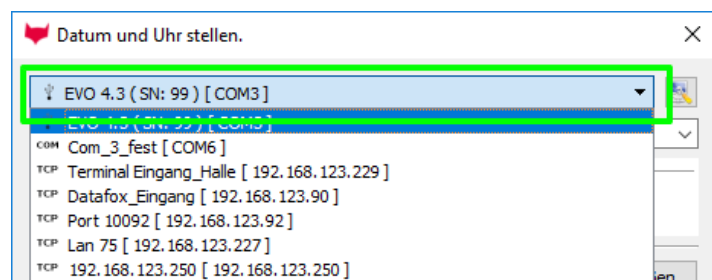
5.8.1.1. Automatische Erkennung über USB für V4 Terminals

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:



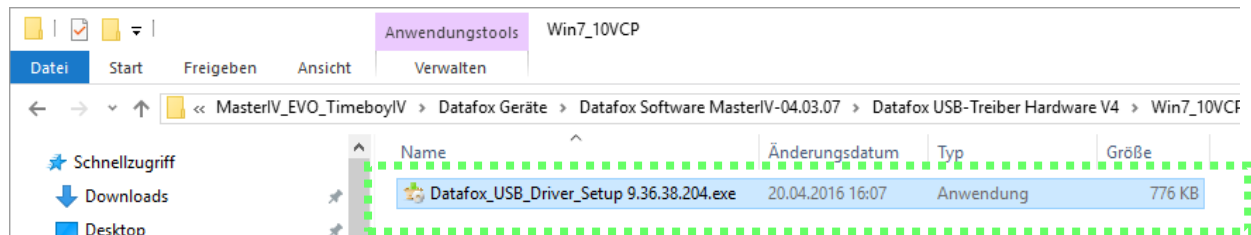
Wenn das Gerät per USB am PC angeschlossen ist, erfolgt keine Kommunikation über eine andere Schnittstelle wie Mobilfunk, IP etc.

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

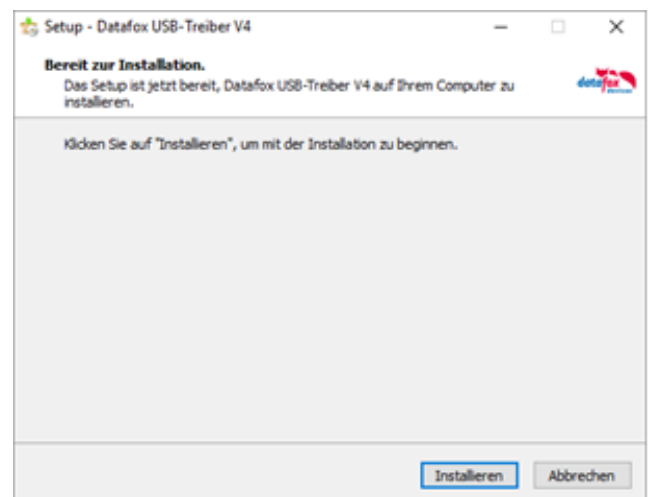
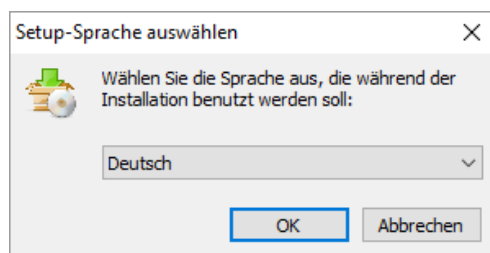
5.8.1.2. USB Treiberinstallation für Datafox Geräte HW V4

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.

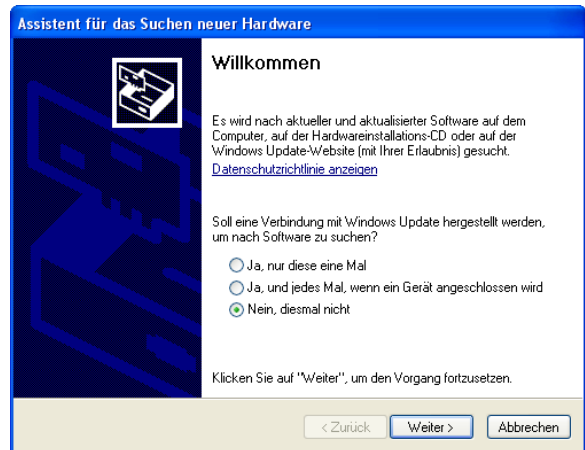


Hinweis:

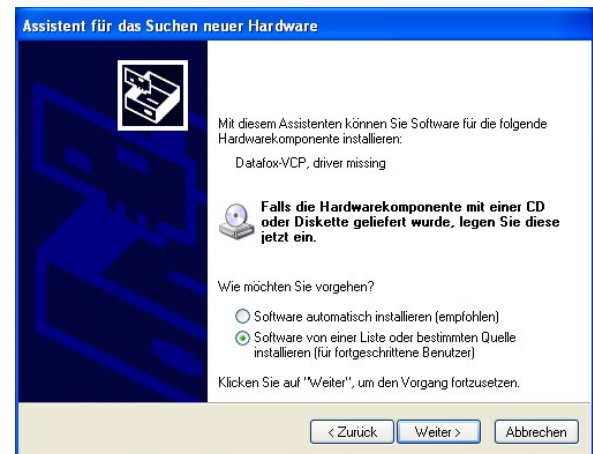
Bei der Installation der Software „DatafoxStudioIV“ wird am Ende der gleiche Treiber automatisch mit installiert.

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

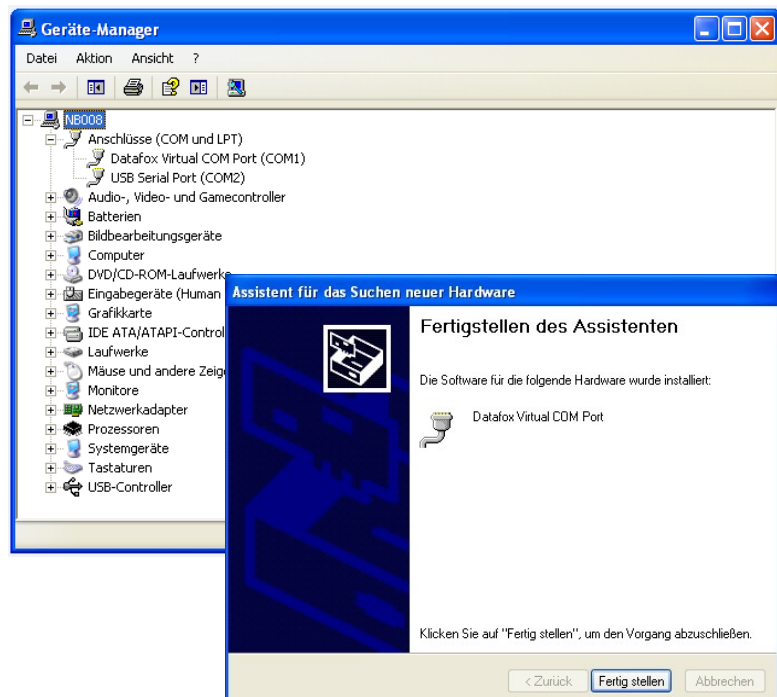
Wählen Sie den Ordner aus, in dem sich der mitgelieferte Treiber befindet.



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.




5.8.2. Kommunikation über USB-Stick (Host)

Um Daten von dem Gerät auf einen USB- Stick übertragen zu können, muss das Gerät über die Option „USB-Host“ verfügen. Sie sehen dies an diesem Ausschnitt.



Der Stick muss in **FAT(32)** formatiert sein.



Der USB- Stick wird automatisch erkannt. Hierzu muss die Hauptkommunikation auf USB-Host stehen. Sie sehen die direkt im Display an diesem Symbol (Icon) . Umstellen können Sie die Kommunikation im Biosmenü des Gerätes.

USB - Stick konfigurieren:

Der USB-Stick wird mit Hilfe des Datafox-StudioIV konfiguriert. Sie finden den Menüpunkt im StudioIV unter „Konfiguration“->USB-Stick konfigurieren. Weitere Erläuterungen finden Sie im Handbuch DatafoxStudioIV.



Hinweis:

Wir empfehlen die Verwendung eines Passwortes für die Kommunikation zwischen USB-Stick und Gerät.



Achtung:

Die USB - Verbindung zum PC darf nicht gleichzeitig mit dem Lesen des USB - Sticks erfolgen. Entfernen Sie das Verbindungskabel USB- zum PC.



Achtung:

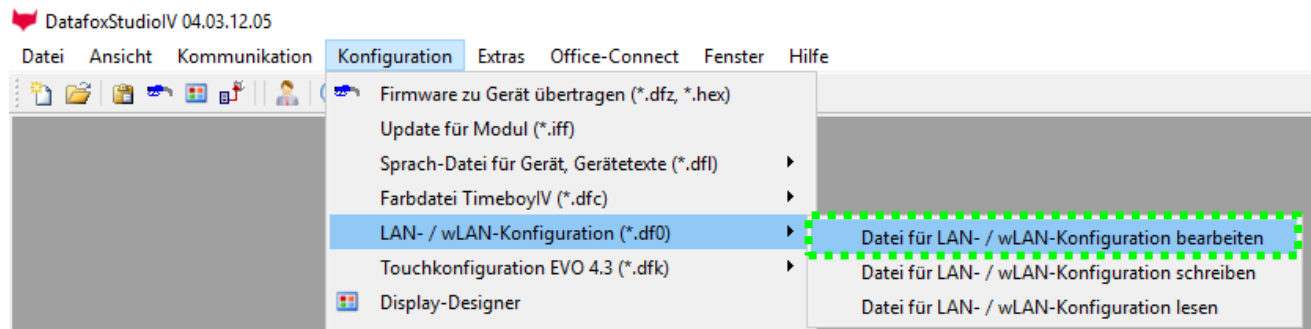
Listen der Zutrittskontrolle können einzeln übertragen werden, Bedienungslisten müssen immer komplett übertragen werden. D.h. alle im Listen die im Gerät über das Setup definiert wurden, müssen auf dem Stick vorhanden sein.

5.8.2.1. Fehlermeldungen bei USB-Stick (Host)

Fehlercode	Bitte diese Tabellen verwenden
1	Fehler beim Lesen
2	Fehler beim Schreiben
3	Fehler in der Kommunikation, keine Antwort vom USB Host
4	Fehler beim Verzeichniswechsel
5	Fehler beim Prüfen auf USB Stick
6	Fehler bei der Suche eines Verzeichnisses
7	Fehler beim Anlegen eines Verzeichnisses
8	Fehler beim Handle aushandeln
9	Fehler beim Öffnen einer Datei war das Verzeichnis nicht vorhanden
10	Fehler der Pfad ist ungültig
11	Fehler Datei bereits geöffnet
12	Fehler beim Öffnen der Datei
13	Fehler beim Schließen der Datei
14	Fehler beim Schließen der Datei, Handle falsch
15	Fehler beim Prüfen des Handles, Handle außerhalb des gültigen Bereichs
16	Fehler beim Prüfen des Handles, Datei ist nicht offen
17	Fehler Datei ist schreibgeschützt
18	Fehler Datensatzbeschreibung des Daten ist ungültig
19	Fehler beim Firmwareupdate
20	Fehler kein USB Stick angeschlossen
21	Falsches Kommunikationspasswort
22	Keine Listen

5.8.3. Kommunikation über TCP / IP

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

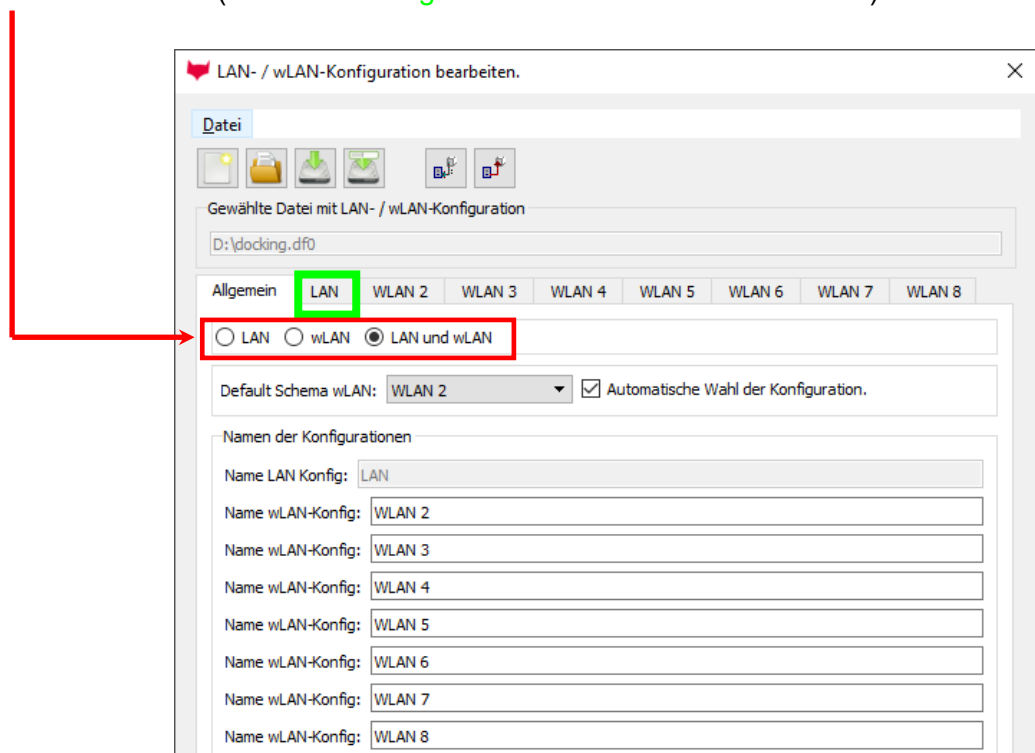


Die LAN / WLAN Konfigurationen werden in einer Datei mit der Endung „*.df0“ abgelegt. Hier haben Sie nun die Möglichkeit die Datei zu bearbeiten, in das Datafox-Gerät zu laden (hochladen) oder aus dem Gerät zu lesen (runterladen).

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)

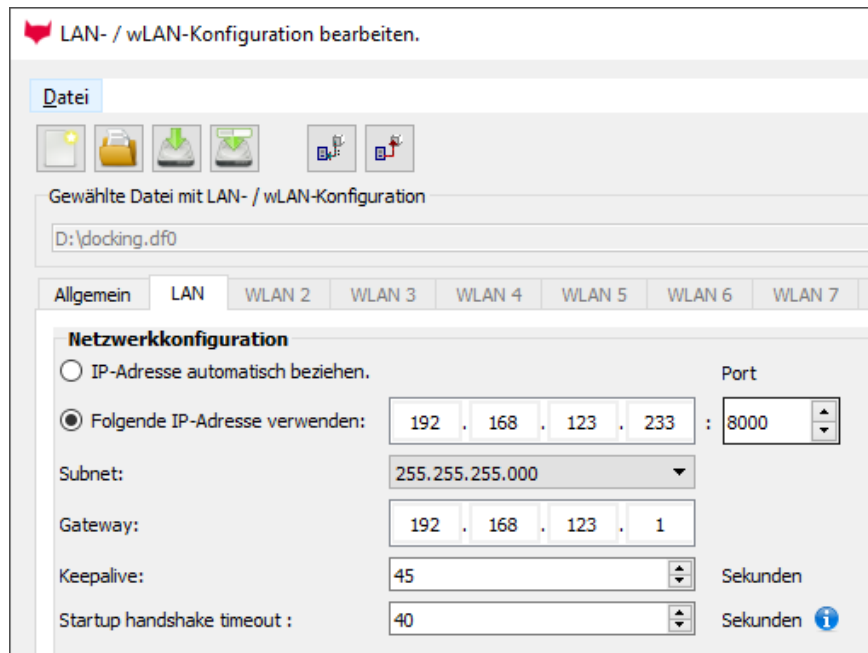


Achtung: Für TimeboyIV gilt, es darf nur die Einstellung wLan genutzt werden.

5.8.3.1. 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.



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“.

5.8.3.2. 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-Parame-
ter haben Sie ein Info-Menü „Modul In-
formationen“.



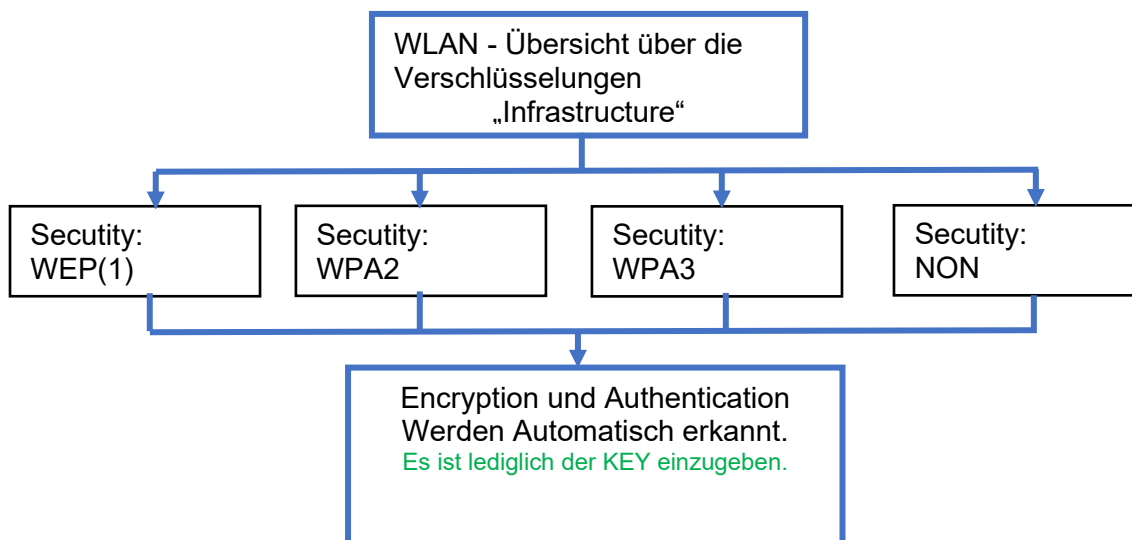
5.8.3.3. M111_WLAN ESP32-c3 ML01 (wLAN-Modul DF-WL03)

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.

5.8.3.4. Texas Instruments TI-CC3135 (Generation 2)

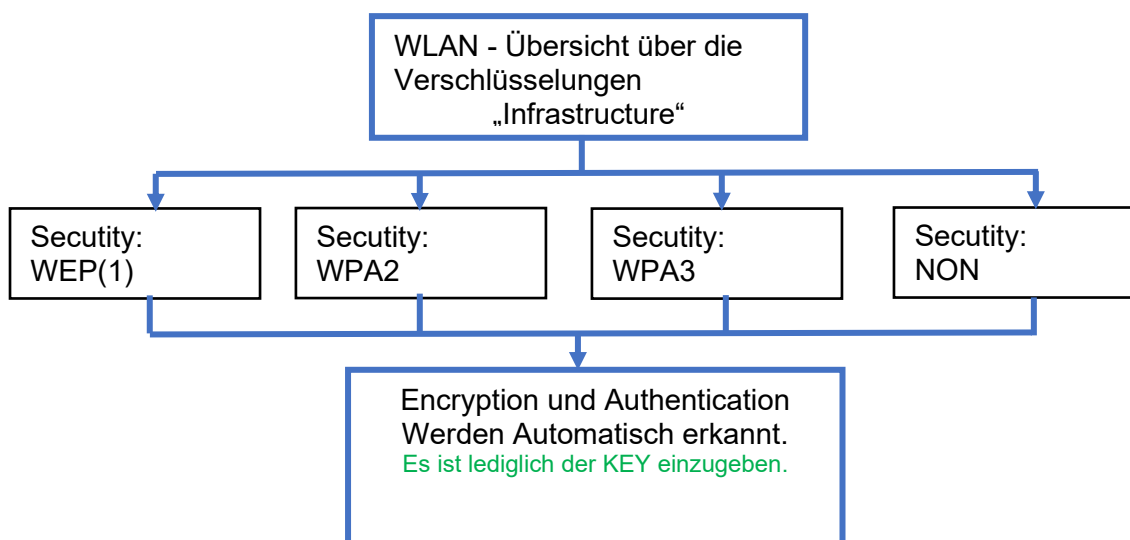
Diese Übersicht zeigt Ihnen, welche WLAN Verfahren unterstützt werden.

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.

5.8.3.5. Redpine (Generation 1)

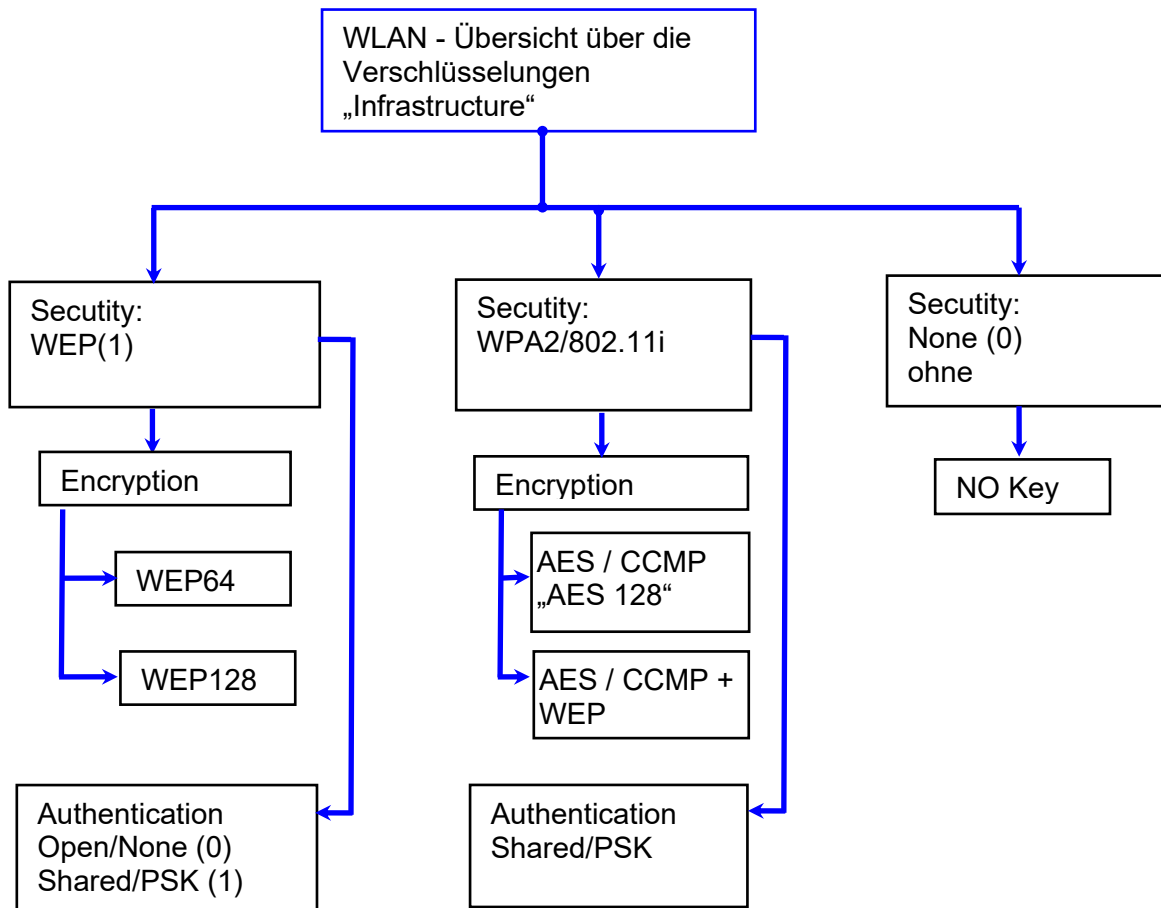
Diese Übersicht zeigt Ihnen, welche WLAN Verfahren unterstützt werden.

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/multiple-input_multiple-output) (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

Bei der Einstellung der Verschlüsselung AES oder WEP wird immer nur eine Art verwendet. Die Einstellung AES+WEP bedeutet bei machen 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.

5.8.3.6. 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', 'Netzwerkconfiguration', 'wLAN-Konfiguration', 'wLAN-Netzwerksicherheit', and 'Optionen'. Annotations include red arrows pointing to the location dropdown menu, the IP address input fields, and the key field. A blue arrow points to the 'Power Save aktivieren' checkbox in the 'Optionen' section. A green dashed box highlights the 'Optionen' section.

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.

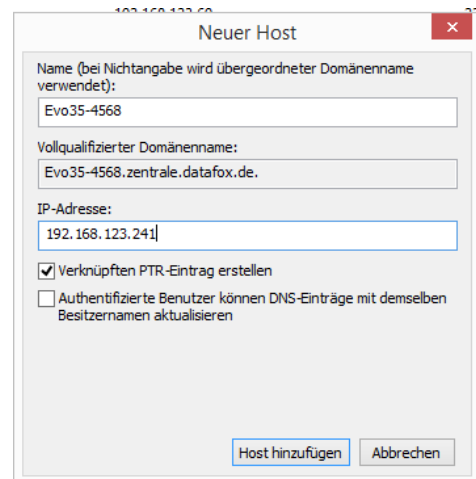
Hinweis:
 Bei automatischer Wahl der Konfiguration / Standort, wird immer zuerst versucht, die Verbindung mit dem Default-Schema aufzubauen.

5.8.3.7. Verbindung der Terminals via TCP/IP DNS / DHCP

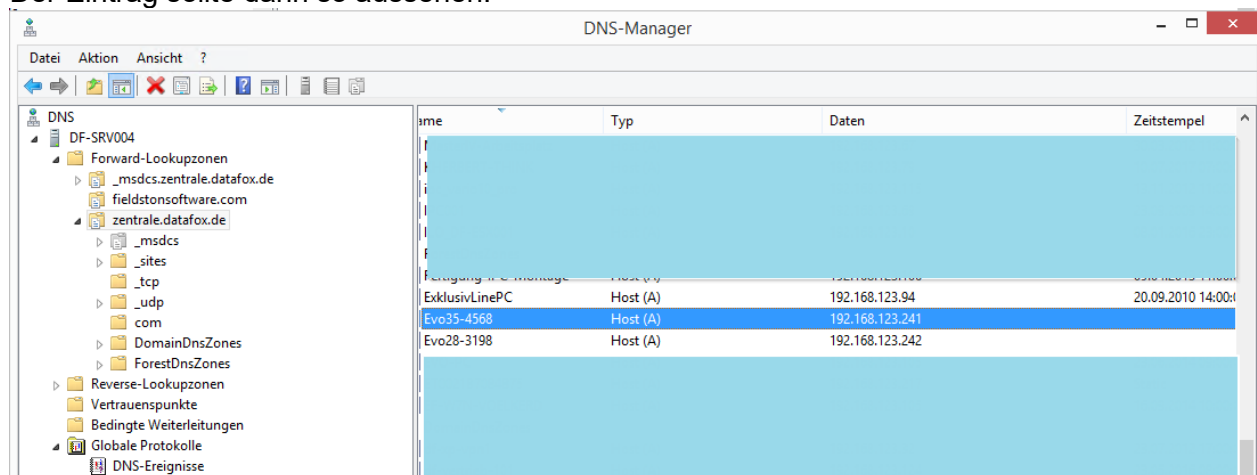
Um ein Datafox EVO-Gerät über den Hostname zu erreichen sind zunächst einige Einstellungen im DNS-Server notwendig. (In unserem Beispiel Fall Windows-Server 2012)

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.

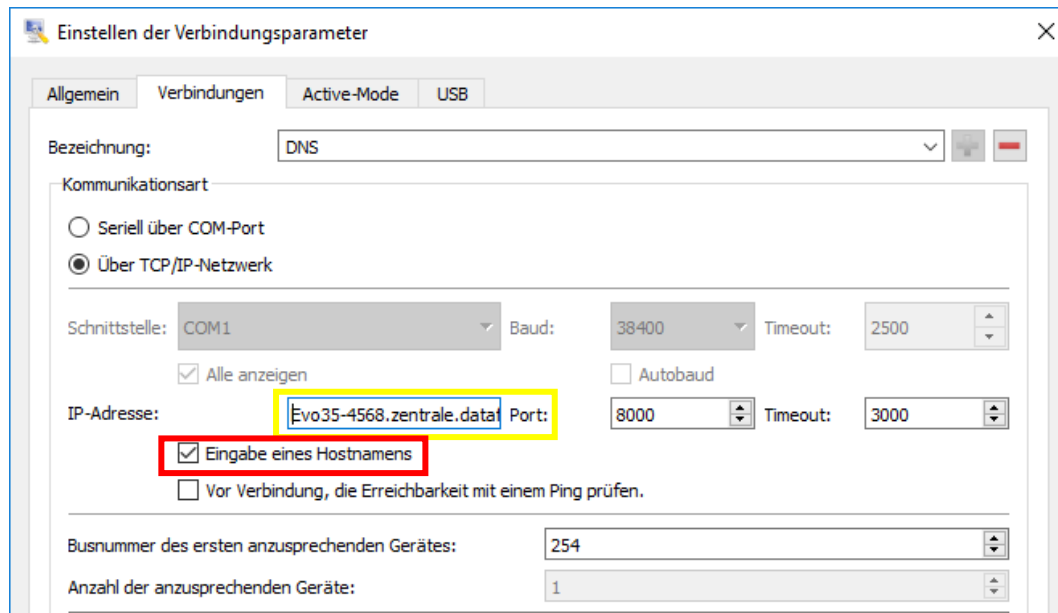


Der Eintrag sollte dann so aussehen:



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	
Evo28-3198	Host (A)	192.168.123.242	

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:

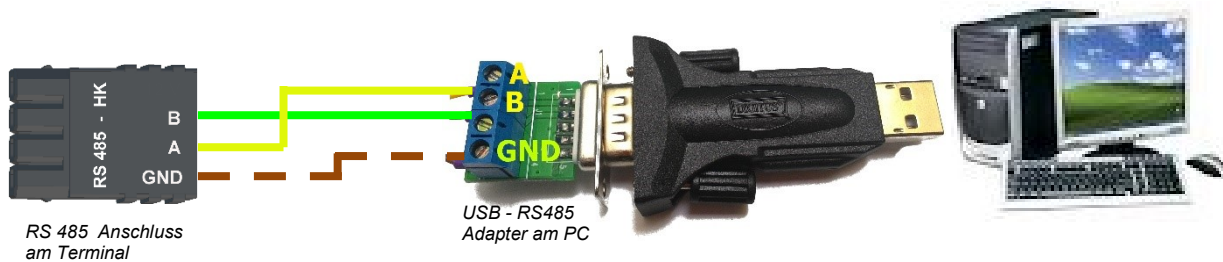
Gerät	Seriennummer	Domain	DHCP- Eintrag
EVO 2.5	10245	.zentrale.de	Evo25-10245.zentrale.de
EVO 3.5	10246	.zentrale.de	Evo35-10246.zentrale.de
AE-Master	10247	.zentrale.de	AE-10247.zentrale.de
PZE-Master	10248	.zentrale.de	PZE-10248.zentrale.de
EVO 4.3	10249	.zentrale.de	Evo43-10249.zentrale.de

5.8.4. Kommunikation der V4 Terminals über RS485

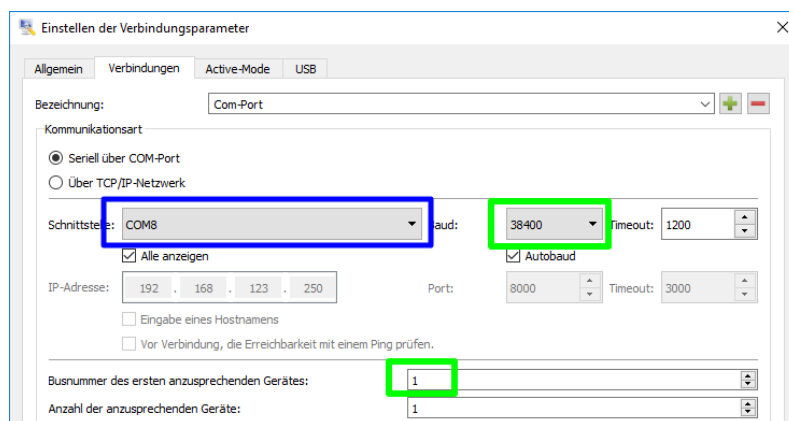
5.8.4.1. Anschluss RS485 zum PC



RS 485 zum PC
bis 1000m



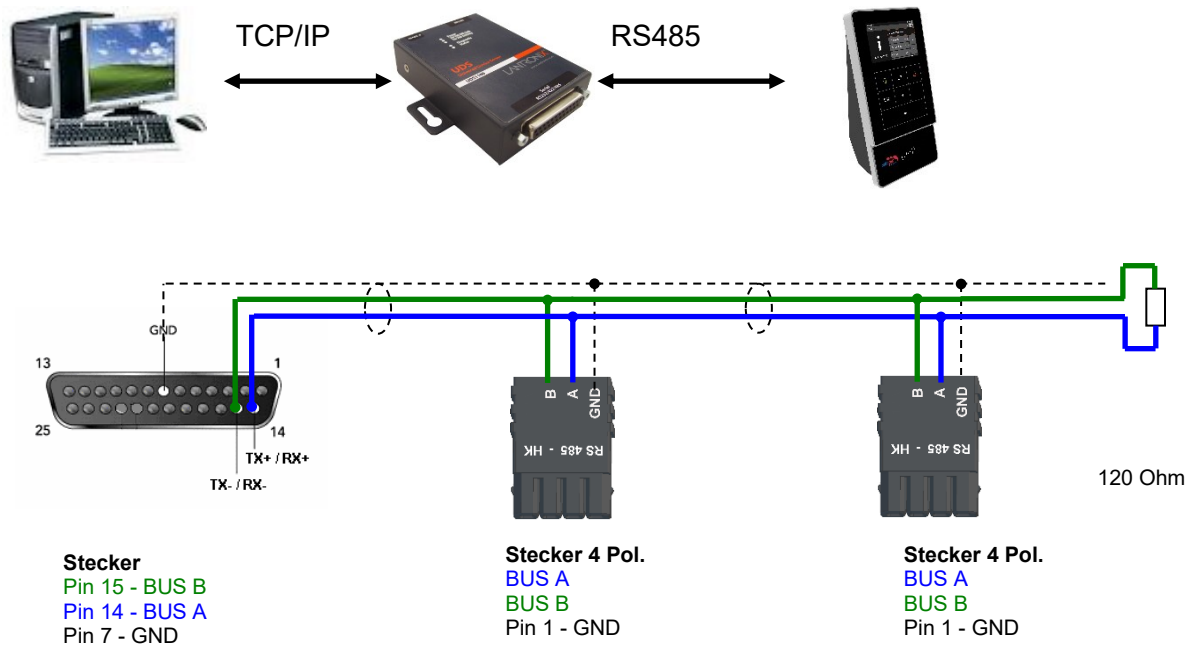
Passende Einstellung im DatafoxStudioIV für die Verbindung über RS 485:



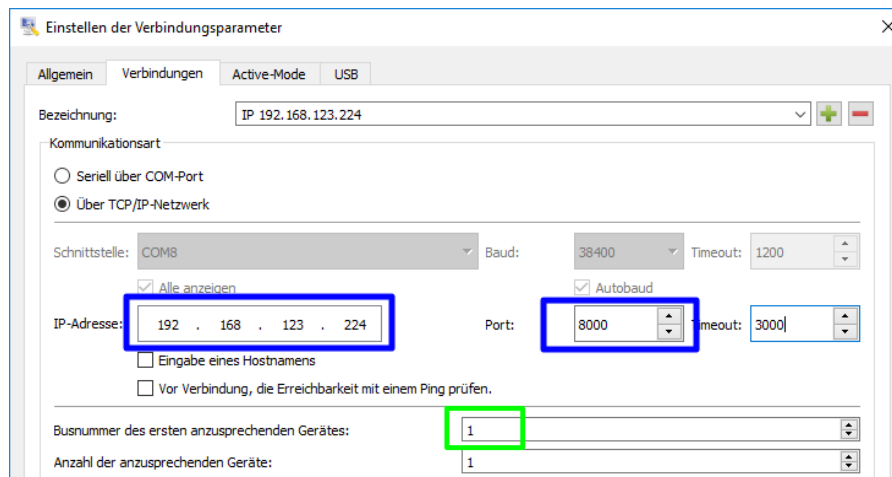
COM-Port
Siehe Geräte-Manager

Baudrate und Busnummer sind am Gerät im Bios-Menü einzustellen.

5.8.4.2. Anschluss EVO Terminal an RS485 über Comserver Lantronix



Passende Einstellung im DatafoxStudioIV für die Verbindung über RS 485:



IP und Port sind am Comserver einzustellen.

Baudrate 38400 und Busnummer sind am Gerät im Bios-Menü einzustellen.

Passende Einstellung im Comserver für die Verbindung über RS 485:

Port: hier als Beispiel 8000

Endpoint Configuration:

Local Port: Auto increment for active connect

Remote Port: Remote Host:

Common Options:

Telnet Com Port Cntrl: Connect Response:

Terminal Name: Use Hostlist: Yes No LED:

IP: hier als Beispiel 192.168.123.224

- [Home](#)
- Network
- [Server](#)
- [Serial Tunnel](#)
- [Hostlist](#)
- [Channel 1](#)
- [Serial Settings](#)
- [Connection](#)
- [Apply Settings](#)

Network Settings

Network Mode:

IP Configuration

Obtain IP address automatically

Auto Configuration Methods

BOOTP: Enable Disable

DHCP: Enable Disable

AutoIP: Enable Disable

DHCP Host Name:


Use the following IP configuration:

IP Address:

Subnet Mask:

Default Gateway:

DNS Server:



Firmware Version: V6.8.0.2

MAC Address: 00-20-4A-FB-91-B1

- [Home](#)
- [Network](#)
- [Server](#)
- [Serial Tunnel](#)
- [Hostlist](#)
- Channel 1
- Serial Settings
- [Connection](#)
- [Apply Settings](#)

Serial Settings

Channel 1

Disable Serial Port

Port Settings

Protocol: Flow Control:

Baud Rate: Data Bits: Parity: Stop Bits:

5.8.5. Kommunikation über Mobilfunk

Der EVO 2.8 Pure kann mit einem Mobilfunkmodem ausgerüstet sein. Damit ist die Kommunikation über das Mobilfunknetz möglich. Die Antenne befindet sich im Anschlussbereich des Gerätes und kann optional bei schlechtem Empfang durch eine externe Antenne ersetzt werden. Die SIM-Karte wird über den Anschlussbereich des Gerätes eingesteckt.

Einsetzen der SIM-Karte beim EVO 2.8




Einsetzen der Sim-Karte beim Gerät

Die SIM-Karte muss in dieser Lage in das Gerät eingesteckt werden.

Achten Sie auf die abgeschrägte Kante.

- Achtung:**
- ! Zum Einschieben ist ein Hilfsmittel in Form eines Stiftes oder Schraubendrehers notwendig. Achten Sie unbedingt darauf, dass Sie die SIM-Karte dabei nicht beschädigen.

Zum Herausnehmen muss die Karte noch etwas weiter eingedrückt werden. Nach dem Loslassen steht sie etwas über, so dass sie entnommen werden kann.

- Hinweis:**
-  Wir empfehlen T-Mobile oder Vodafone als Provider für Mobilfunk einzusetzen! Unsere Erfahrung zeigt, dass bei anderen Anbietern mit häufigeren Einwahlen und damit auch verzögerter Datenübertragung und ggf. mit höheren Kosten gerechnet werden muss.

Informationen zu M2M:

http://www.t-mobile.de/business/machinetomachine/m2m-im-einsatz/0,23219,26762-_,00.html

5.8.5.1. Statusmeldungen für Mobilfunk am Display

Den Status der GPRS-/GSM-Verbindung kann man jederzeit in der Statusleiste am Display ablesen.

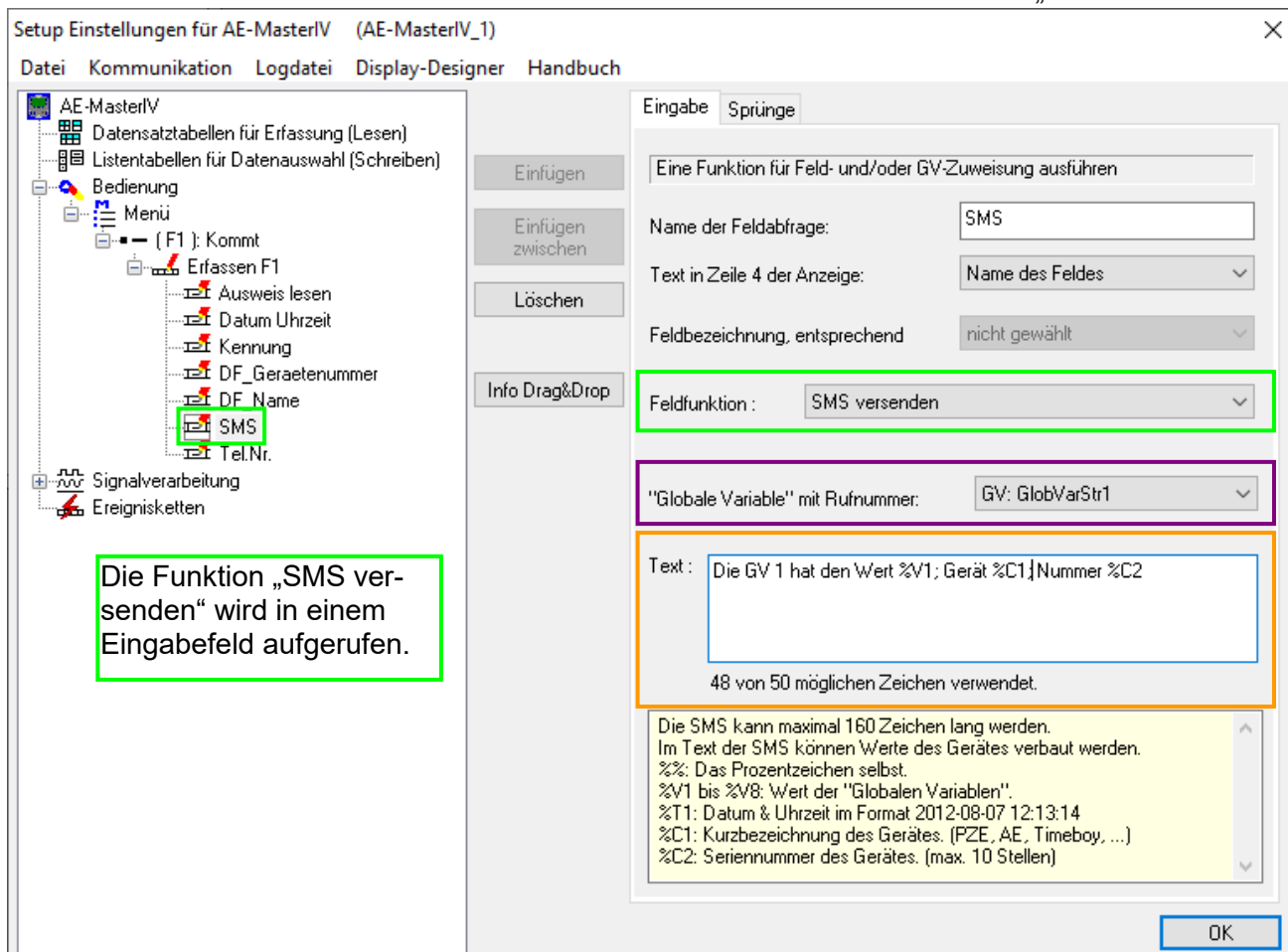
Pin	Bez.
0	Modem ist AUS
1	Initialisierung der Software
2, 3	Starten des Modems
4, 5	Initialisierung des Modems und SIM-Karten Prüfung
6	Falls PIN erforderlich, senden der PIN
7	Falls PUK erforderlich, senden der PUK
8	Erweiterte Initialisierung des Modems
9	Bios-Modus
10	Modem in Standby
12	Rufannahme
14	GSM Verbindung aktiv
15, 16	GSM Verbindung beenden
20	GPRS Standby, Einwahl erst, wenn Daten vorliegen
25	Verbindungsaufbau zum Provider (Attach)
30	GPRS Standby (warte auf Daten)
31	Verbindungsaufbau zum Server (Open)
32	Verbindung besteht zum Server (warte auf Daten)
33	Sende Daten an Server (HTTP)
34	Warte auf Quittung vom Server (HTTP)
35	Paket empfangen (TCP/IP)
36	Paket senden (TCP/IP)
37	Verbindungsabbau (Close)
38	Wartepause zwischen Verbindungsaufbauversuchen bei Active Mode
40	Sendepause nach Verbindungsfehler bis zu 15 Minuten
41 ¹⁾	Sendepause nach wiederholtem Verbindungsaufbau zum Provider bis zu 15 Minuten
42 ¹⁾	Kontingent zum Verbindungsaufbau für diesen Tag aufgebraucht
43	Im Gerät ist die http-Verschlüsselung aktiviert, im Server nicht
44	Akkuspannung zu niedrig, Modem abgeschaltet
45	Verbindung zum Provider nicht möglich bzw. Roaming nicht möglich
50	Verbindungsabbau mit Provider
55	Abschalten des Modems

5.8.6. Kommunikation per SMS

5.8.6.1. SMS versenden

Der EVO 2.8 Pure, der mit einem GPRS-Modem ausgestattet ist, ist in der Lage eine SMS zu senden. Voraussetzung dafür ist, dass die Hauptkommunikation auf „GPRS“ eingestellt ist.

Dazu wurde in der Parametrierungssoftware DatafoxStudioIV eine neue Feldfunktion „SMS versenden“



hinzugefügt. Siehe Bild:

Die SMS kann maximal 160 Zeichen lang werden.
 Im Text der SMS können Werte des Gerätes verbaut werden.
 %%: Das Prozentzeichen selbst.
 %V1 bis %V8: Wert der Globalen Variablen.
 %T1: Datum - Uhrzeit im Format 2012-08-07 12:13:14
 %C1: Kurzbezeichnung des Gerätes. (PZE, AE, TIMEBOY, ...)
 %C2: Seriennummer des Gerätes. (max. 10 Stellen)

Die Rufnummer, an die diese Nachricht gesendet werden soll, wird in einer GV (globalen Variablen) angegeben.



Achtung:

Geben Sie die Rufnummer immer mit einer Landesvorwahl an.
 Bsp.: +49161458*****

Es werden bis zu 128 SMS im Gerät gespeichert. Kommt dann eine weitere hinzu, wird die älteste SMS gelöscht (Ringspeicher).

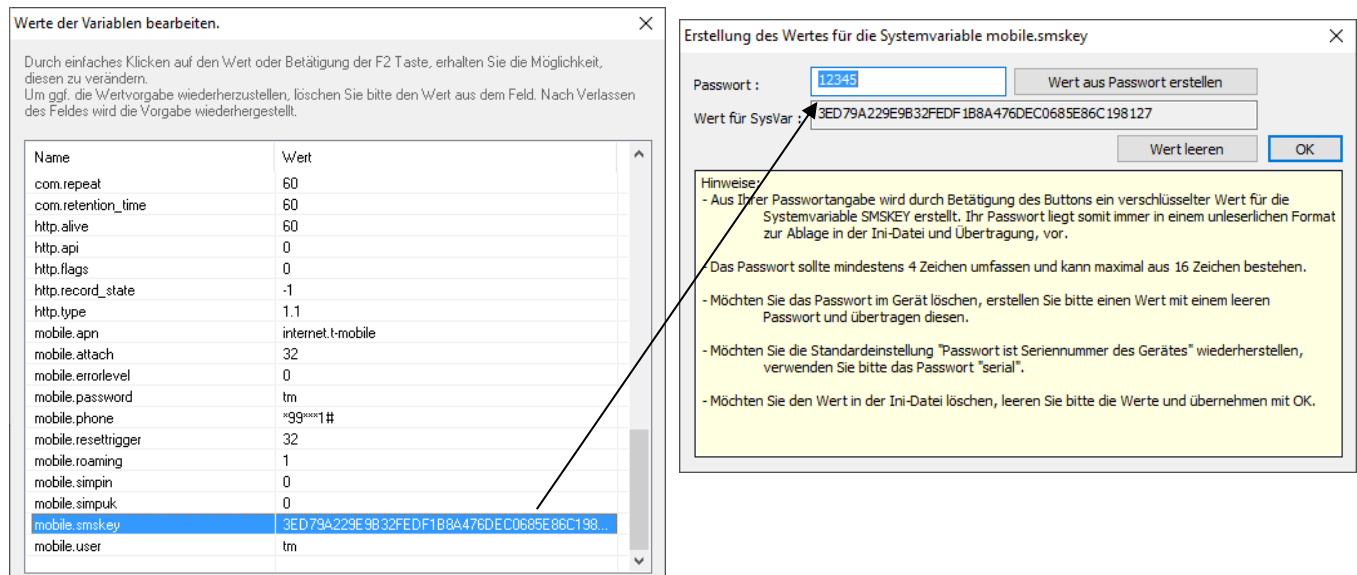
5.8.6.2. SMS empfangen

Datafox MasterIV-Geräte, die mit einem GPRS-Modem ausgestattet sind, sind nun in der Lage eine SMS zu empfangen.

Folgende Funktionen können dadurch realisiert werden:

- ▶ Anzeige, einer an das Gerät gesendeten SMS auf dem Display, wie es bereits durch DFCComSendMessage oder bei der HTTP-Rückantwort möglich ist.
- ▶ Aufforderung eine Serviceverbindung aufzubauen (identisch zur HTTP-Antwort)
- ▶ Eine Eingabekette in der Signalverarbeitung starten
- ▶ Einen Signalton ausgeben

Bedingung eine SMS zu empfangen ist, dass ein **KEY** in dem SMS-Text hinterlegt sein muss. Der Key für das Gerät, wird in der GPRS/HTTP .ini Datei hinterlegt.



Werte der Variablen bearbeiten.

Name	Wert
com.repeat	60
com.retention_time	60
http.alive	60
http.api	0
http.flags	0
http.record_state	-1
http.type	1.1
mobile.apn	internet.t-mobile
mobile.attach	32
mobile.errorlevel	0
mobile.password	tm
mobile.phone	*99***1#
mobile.resettrigger	32
mobile.roaming	1
mobile.simpin	0
mobile.simpuk	0
mobile.smskey	3ED79A229E9B32FEDF1B8A476DEC0685E86C198...
mobile.user	tm

Erstellung des Wertes für die Systemvariable mobile.smskey

Passwort :

Wert für SysVar :

Hinweise:

- Aus Ihrer Passwortangabe wird durch Betätigung des Buttons ein verschlüsselter Wert für die Systemvariable SMSKEY erstellt. Ihr Passwort liegt somit immer in einem unleserlichen Format zur Ablage in der Ini-Datei und Übertragung, vor.
- Das Passwort sollte mindestens 4 Zeichen umfassen und kann maximal aus 16 Zeichen bestehen.
- Möchten Sie das Passwort im Gerät löschen, erstellen Sie bitte einen Wert mit einem leeren Passwort und übertragen diesen.
- Möchten Sie die Standardeinstellung "Passwort ist Seriennummer des Gerätes" wiederherstellen, verwenden Sie bitte das Passwort "serial".
- Möchten Sie den Wert in der Ini-Datei löschen, leeren Sie bitte die Werte und übernehmen mit OK.

Textnachricht

Das Schlüsselwort welches in der SMS enthalten sein muss ist

message=Text1↵ Text Zeile2 ↵ Zeile3 usw.

&delay=10&key=12345

Hierbei bedeutet die 10, dass die Nachricht für 10 Sekunden angezeigt wird. Nach dem ↵ Zeichen wird jeweils automatisch ein Zeilenumbruch eingefügt. Wurde noch kein key im Gerät hinterlegt, muss die Seriennummer des Gerätes als key verwendet werden. Wird der key im Gerät gelöscht (leeres Passwort), so wird jede SMS angenommen.

Die jeweils letzte Nachricht können Sie im Bios-Menü unter „Allgemeine Informationen einsehen.

Serviceverbindung

Der Inhalt der SMS ist analog zu dem der HTTP-Antwort vom WEB-Server. Bisher werden 3 Schlüsselworte unterstützt: **service**, **host** und **port**. Dem Schlüsselwort muss ein ‚=‘-Zeichen mit dem jeweiligen Wert folgen. Die einzelnen Felder wiederum werden mit dem ‚&‘-Zeichen getrennt. Mit dem Schlüssel **&service=1**, wird das Gerät veranlasst, eine Wartungsverbindung aufzubauen. Es wird versucht zu dem im Studio unter „Konfiguration->Systemvariablen Active-Mode“ eingestellten Server („Host“ und „Port“) eine Verbindung herzustellen. Optional ist es auch möglich, den Server direkt in der SMS anzugeben -> **host=**. Voreingestellt ist dann der Port 8000. Mit dem zusätzlichen Parameter **port=** kann auch dieser Wert in jeder SMS angepasst werden.

“&service=2“

Achtung ! ist erst ab der Hardware V4 mit GPRS(Mobilfunk) mit FW 04.03.06.XX möglich.

Bei der Verwendung von dem Parameter 2 wird die Serviceverbindung sofort aufgebaut.

Beispiele:

- a) **service=X&key=12345**
- b) **service=X&host=www.datafox.de&key=12345**
- c) **service=X&host=123.123.123.123&key=12345**
- d) **service=X&host=www.datafox.de&port=4711&key=12345**
- e)

In Beispiel a) wird zu dem im „Active-Mode“ hinterlegten Server eine Verbindung aufgebaut.

Bei b) und c) werden Verbindungen auf Port 8000 zum jeweils genannten Server aufgebaut.

Im letzten Beispiel wird versucht, eine Verbindung zum Datafox-Server an Port 4711 herzustellen.

Eine Eingabekette in der Signalverarbeitung starten

Das Schlüsselwort, welches in der SMS enthalten sein muss, ist:
ek=Name&key=12345 (der Eingabekette).

Hierbei muss der **Name** der Eingabekette vollständig übereinstimmen, sonst wird diese nicht ausgeführt. Empfängt nun ein Gerät eine SMS mit diesem Text, so wird die Eingabekette ausgeführt. Ist ein Schlüssel hinterlegt, so wird natürlich auch dieser Benötigt **&key=12345**).

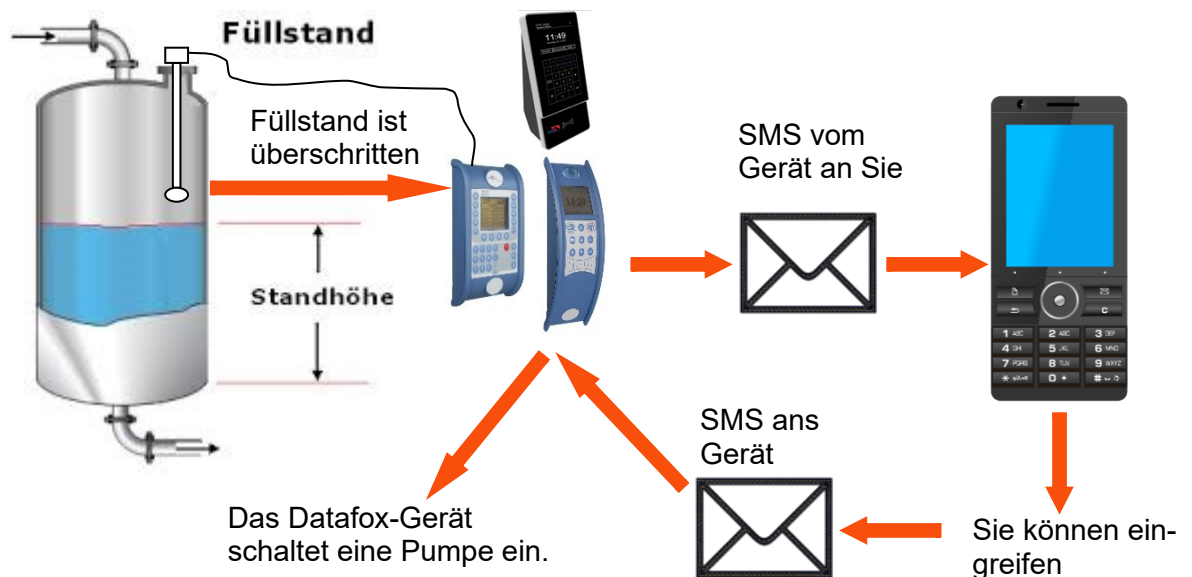
Die Möglichkeiten, die sich dadurch ergeben, sind sehr zahlreich.
 Beispiele:

Mit der SMS kann eine Türöffnung durchgeführt werden.



Überwachungsservice einer technischen Anlage bei Störung oä.

Sollte die Regelung des Füllstandes mal abweichen, kann dies durch eine SMS gemeldet werden. Das Datafox MasterIV soll hier nicht als Regler, sondern nur als Benachrichtigung bei einer Abweichung dienen. Bei Bedarf kann auch ein Eingriff erfolgen.



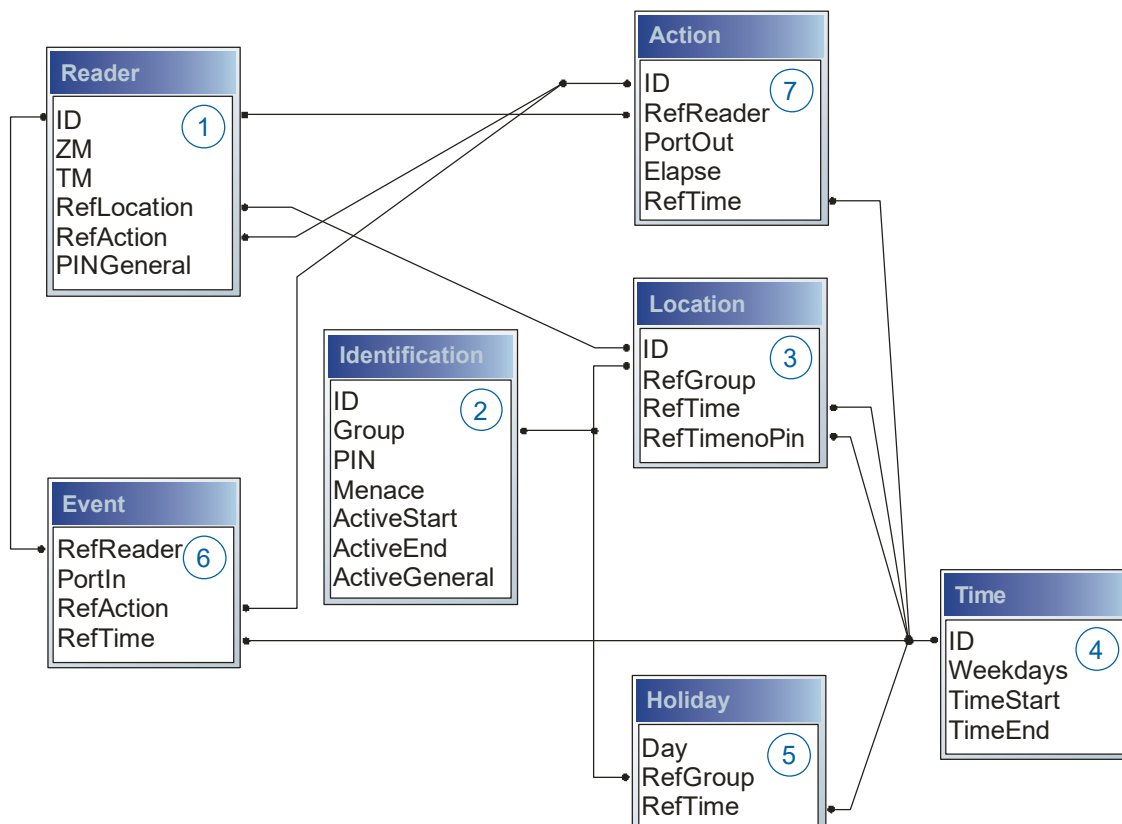
Achtung:

Es gibt keine 100%ige Sicherheit, dass eine gesendete SMS auch beim Empfänger ankommt. Dies ist nur ein Beispiel, welches die Möglichkeiten darstellen soll.

5.9. Anschluss der Zutrittskontrolle

5.9.1. Konfiguration der ZK / Übersicht

Grundlage der Zutrittskontrolle II sind Tabellen. In ihnen werden alle Informationen über die Hardwarekonfiguration des Zutrittskontrollsystem, 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 EVO 2.8 Pure 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

5.9.1.1. 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. ! Aktionen die hier ausgeführt werden, dürfen nicht mit Zutrittsaktionen gemischt werden!

5.9.2. Zutrittskontrolle II mit EVO Intera

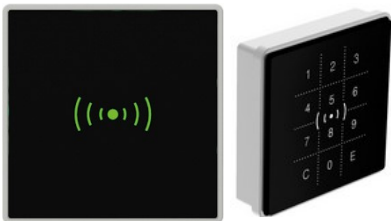
Folgende Hardware steht für den Aufbau einer Zutrittskontrolle mit EVO-Intera zur Verfügung. Entsprechend der Hardwareanforderung der einzelnen Geräte können diese in verschiedenen Varianten miteinander kombiniert werden.

EVO 2.8 Pure



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



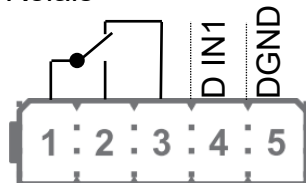
Unterputz: 81 x 81 x 19 mm (BxHxT)

Der EVO-ZK-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.

IO-Modul für EVO Intera



Relais



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.

Anzeige	Beleuchtetes Transpondersymbol	3-farbig weiß, grün, rot	
Individualisierung	Integriertes Leuchtfeld	Individuell bedruckbare Frontscheibe mit Beleuchtungsfeld 56 x 37mm	
Stromversorgung	10 - 30V DC, max. 120mA	Einschaltstrom 250 mA	
Montage	Edelstahl-Montageplatte, Leser wird eingehängt und gesichert.		
Umgebungswerte	Umgebungstemperatur, Schutzart	-20 °C bis +70 °C, IP65	
Transponder Leseverfahren	125kHz	Mifare	Legic
	Hitag 1+2+5	Mifare Classic	Legic prime
	Unique EM4102	Mifare Desfire	Legic advant
	Titan EM4450	Mifare Ultralight	

Anschluss und Kontaktbelegung des EVO-Lesers:



DIP-Schalter:

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

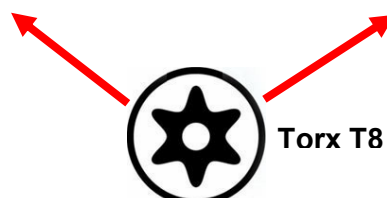
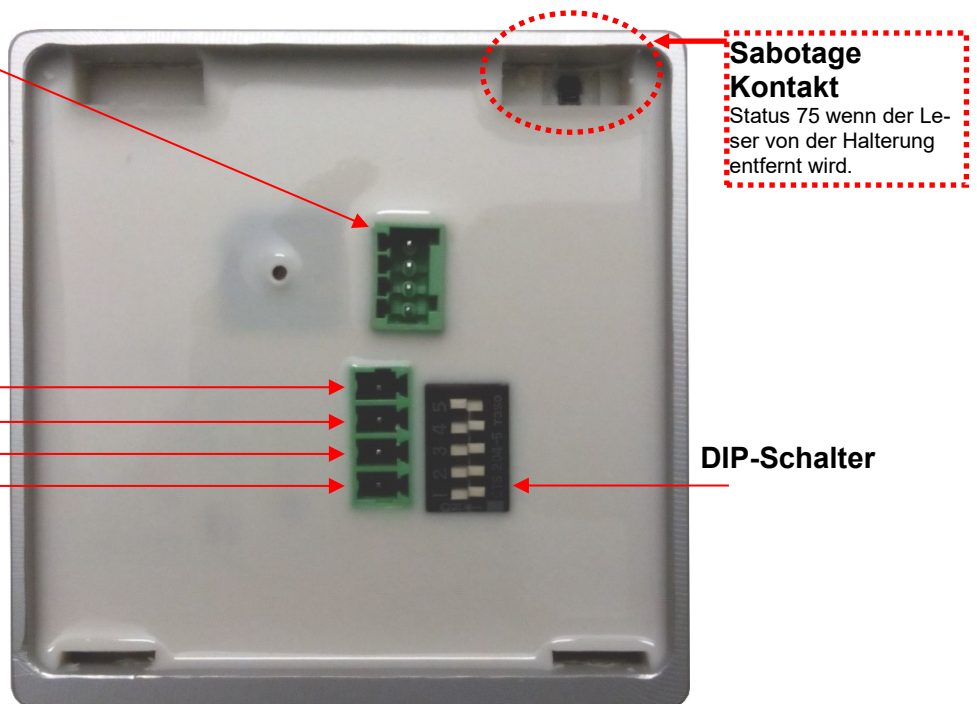
Beispiel	5-4-3-2-1
Adresse 2, mit Abschlusswiderstand	1-0-0-1-0
Adresse 3, ohne Abschlusswiderstand	0-0-0-1-1

Daraus ergibt sich ein Adressbereich von 0 bis 15.

**Anschluss für Tür-
steuerungsplatine**
Relais + Eingang
(später 5pol.)

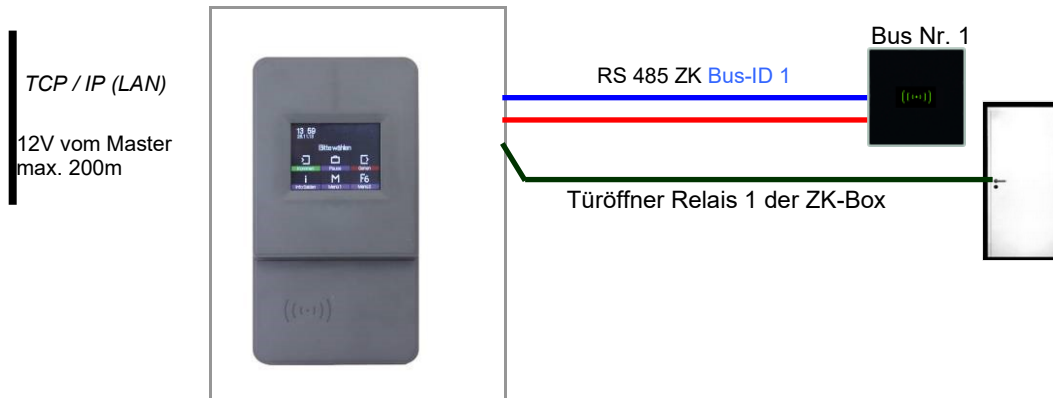
Nr.	Beschreibung
1	+10V bis +30V DC ! neu
2	RS 485-Daten „B“
3	RS 485-Daten „A“
4	GND

**! Bei älteren Lesern
darf die Spannungs-
versorgung max. 16V
betragen. Bei diesen
Lesern fehlt die Span-
nungsangabe auf
dem Typenschild.**



5.9.2.1. Anschluss der EVO Intera

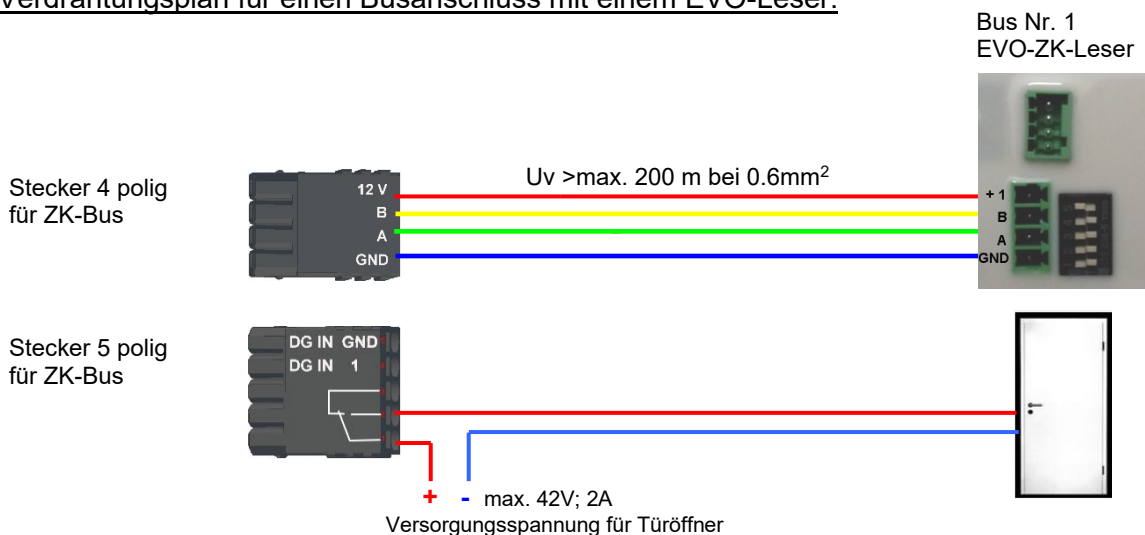
Verkabelungsplan für 1 Türen, 1 Relais in dem EVO 2.8 Pure:



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 EVO-Leser:

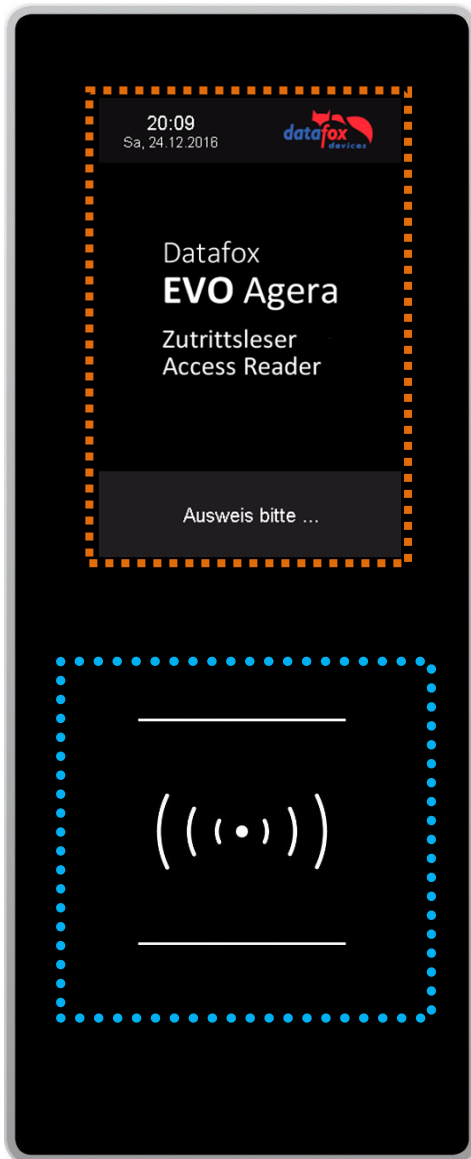


5.9.3. Zutrittskontrolle II mit EVO Agera

5.9.3.1. 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 -**

5.9.3.2. Anzeigen für den ZK-Status

Aktuell gibt es 2 Anzeigen für:

Zutritt gewährt:

Zutritt verweigert:



Datafox Standardbild



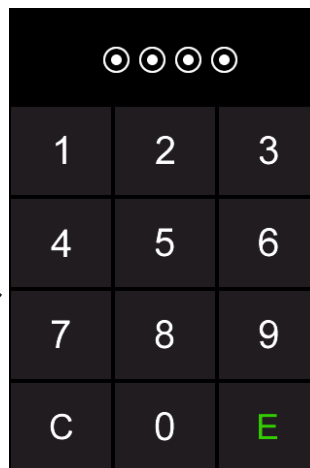
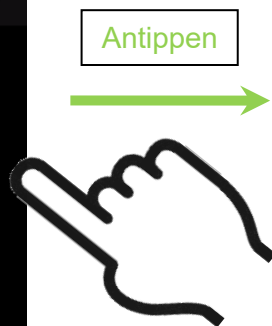
Datafox Standardbild

5.9.3.3. Anzeigen einer PIN-Tastatur

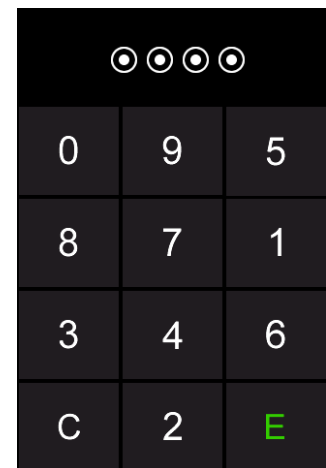
Wenn für den Zutritt noch eine zusätzliche PIN abgefragt wird, wird die Tastatur automatisch eingeblendet. Für den Zutritt nur über die Eingabe einer PIN genügt ein kurzes Antippen um die PIN-Anzeige zu aktivieren.



Datafox Standardbild
Bild 1 der Galerie



Datafox Standardbild
PIN normal



Datafox Standardbild
PIN zufällige Anordnung

5.9.3.4. Fehlerausgaben

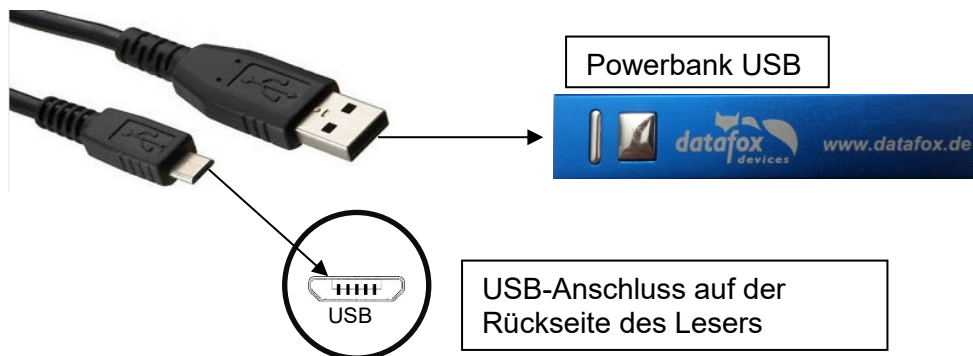
Der Leser steht in ständiger Kommunikation mit dem Master. Für den Fall das die Kommunikation unterbrochen wird, wird dies am Leser mit dem Text:Fehler Kommunikation.



5.9.3.5. 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.



5.9.3.6. 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	

5.9.3.7. 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

5.9.3.8. 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	

5.9.3.9. 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	↵
	←	

5.9.3.10. 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.

5.9.3.11. Anschluss des Agera

Auf der Rückseite befindet sich ein mehradriges Anschlusskabel.

Die Belegung ist dabei wie folgt:

Nr.	Farbe	Funktion
1	Rot	+12V Power Input (10 - 30V DC)
2	Blau	GND Power Input
3	Gelb	RS485 - B
4	Grün	RS485 - A

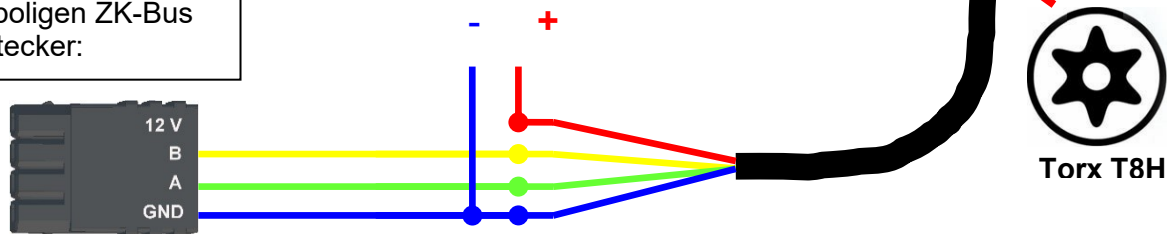
I/O-Erweiterung

Nr.	Farbe	Funktion
5	Weiß	Relais gemeinsam
6	Braun	Relais Schließer
7	Grau	Relais Öffner
8	Violett	DigIn
9	Schwarz	DigIn - GND



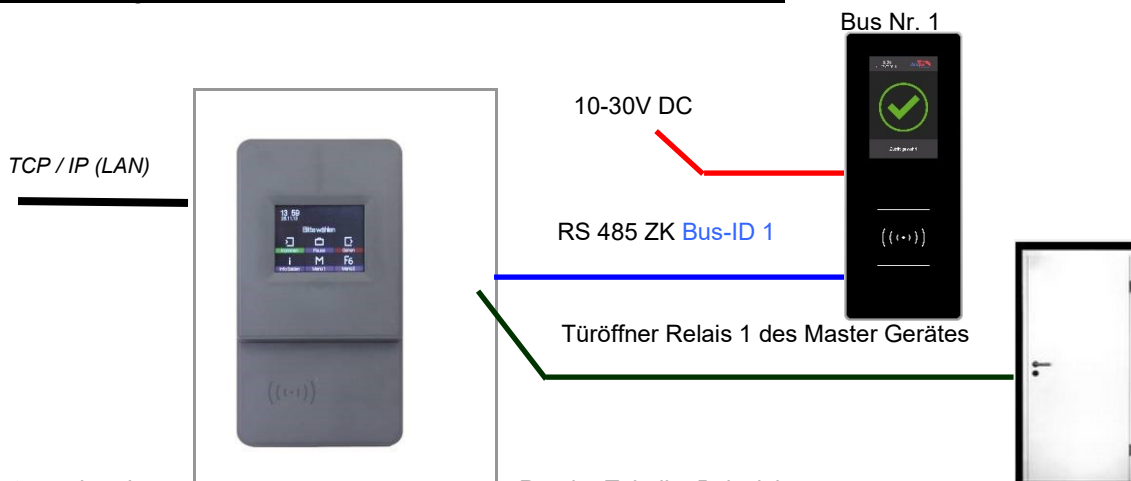
Anschluss an den 4poligen ZK-Bus Stecker:

Spannungsversorgung 12 – 30 V



Gehäuse	Aufbau	Front aus Alu mit gehärtetem Echtglas, kapazitivem Touch, Gehäuserückwand Kunststoff: PC-ABS		
	Abmessungen (Breite x Höhe x Tiefe)	85 mm x 208 mm x 27 mm, ca. 20mm zusätzlich in UP-Dose		
	Gewicht	Basisgerät 550g zzgl. Wandhalterungsblech		
Anzeige	LCD	TFT: 320 x 480 Pixel, active area 49,0 x 73,4 mm mit LED-Backlight		
	Beleuchtetes Transpondersymbol	3-farbig weiß, grün, rot		
Tasten	Art, Größe	Tastatur über kapazitivem Touch-Display, Touchfläche 73,4 x 49,0mm,		
Individualisierung	Individuelle Grafiken	Benutzeranzeigen über Grafiken individuell definierbar		
	Integriertes Leuchtfeld	Individuell bedruckbare Frontscheibe mit Beleuchtungsfeld 56 x 37mm Farbe immer wie Transpondersymbol		
Stromversorgung	10 - 30V DC, max. 500mA			
Montage	Edelstahl-Montageplatte, Leser wird eingehängt und gesichert.			
Umgebungswerte	Umgebungstemperatur, Schutzart	-20 °C bis +70 °C, IP65		
Kommunikation	RS485-Schnittstelle, phg_crypt, 16 Busadressen und Abschluss Widerstand über Menü einstellbar			
Sabotagesensor	Sabotageerkennung über Abstandserkennung zur Wandhalterung			
Optionen	Türmodul	Erweiterungsmodul mit Relais (Umschalter) und einem digitalen Eingang Diese Erweiterung sollte nicht im ungesicherten Bereich eingesetzt werden.		
	Transponder Leseverfahren	125kHz	Mifare	Legic
	Hitag 1+2+5	Mifare Classic	Legic prime	
	Unique EM4102	Mifare Desfire	Legic advant	
	Titan EM4450	Mifare Ultralight		

Verkabelungsplan für 1 Türen, 1 Relais in dem EVO 2.8 Pure:

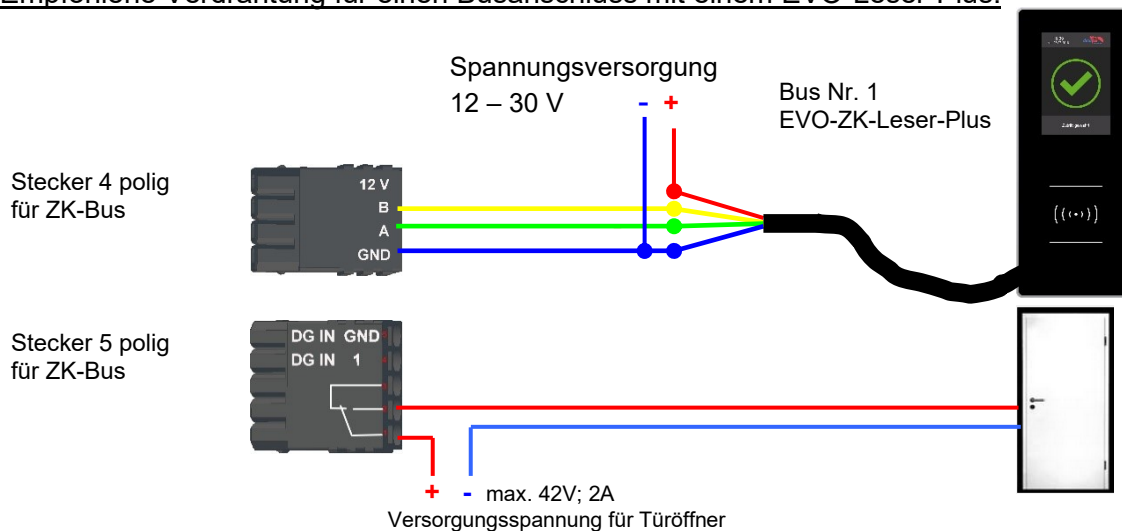


Entsprechende

Reader Tabelle, Beispiel:

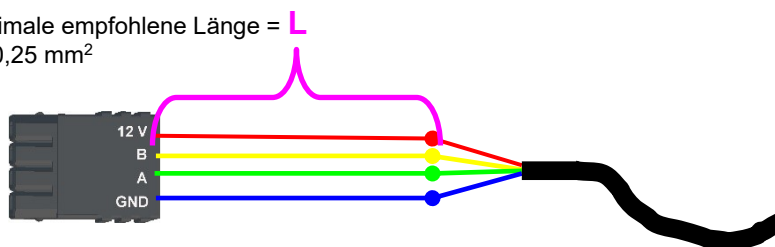
ID	ZM / Bus-ID	TM (Busadresse)	RefLocation	RefAction	PinGeneral	Beschreibungstext
1	1	010	1	1	0	Leser an RS485 Modulplatz 1 = Bus ID 1
4	1	320	0	1	0	ZK-Box V4 (Mastergerät)

Empfohlene Verdrahtung für einen Busanschluss mit einem EVO-Leser-Plus:



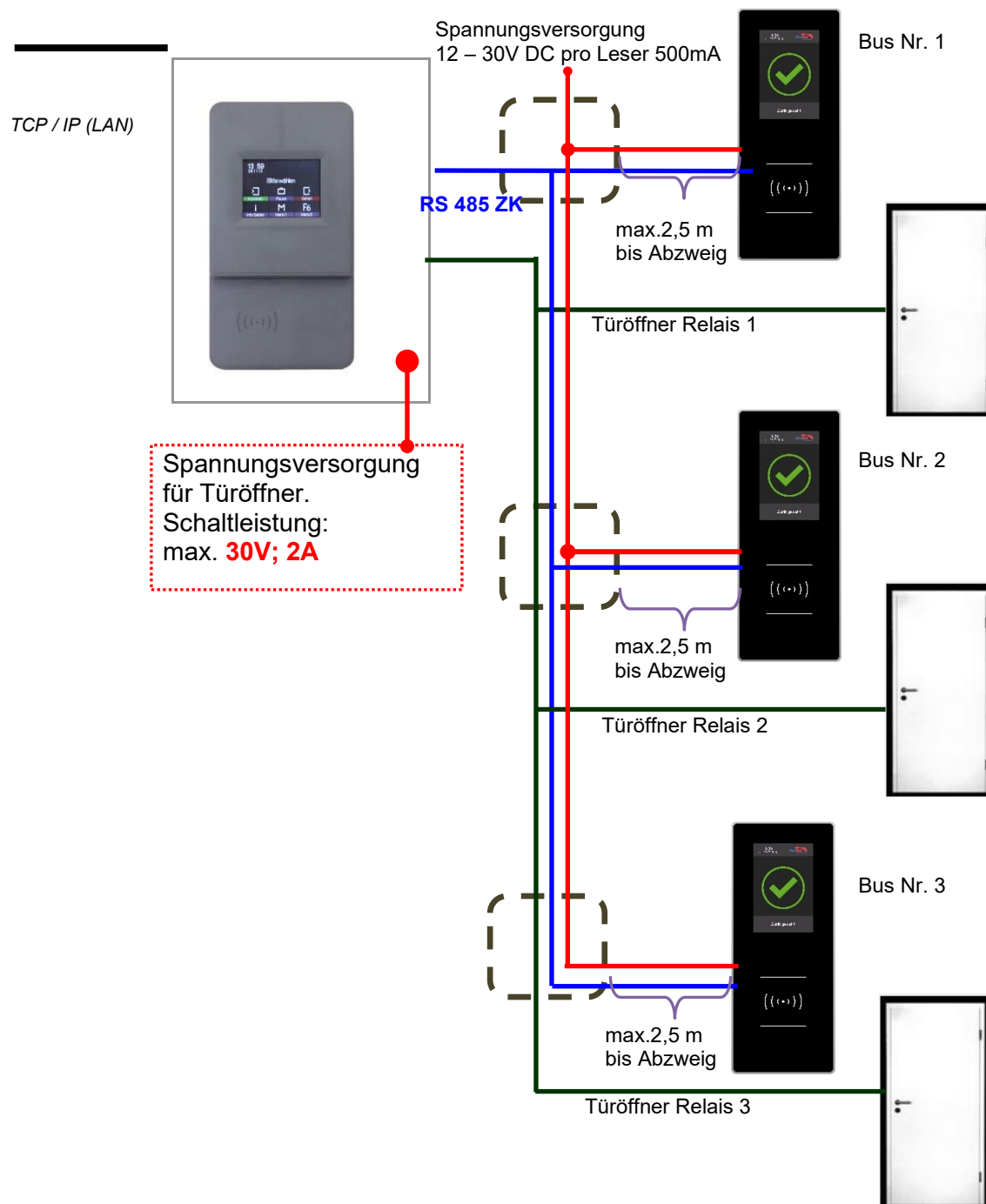
Alternativ kann bei der Verwendung von **nur einem Leser** dieser an die Spannungsversorgung des RS485 Moduls aus dem Master genutzt werden.

Maximale empfohlene Länge = L
mit 0,25 mm²



Leser Typ	L in m	Strom in mA	Strom bei Start in mA	gf. Ergänzungen
Legic	50	iA	iA	
Mifare	100	iA	iA	
Unique	100	iA	iA	

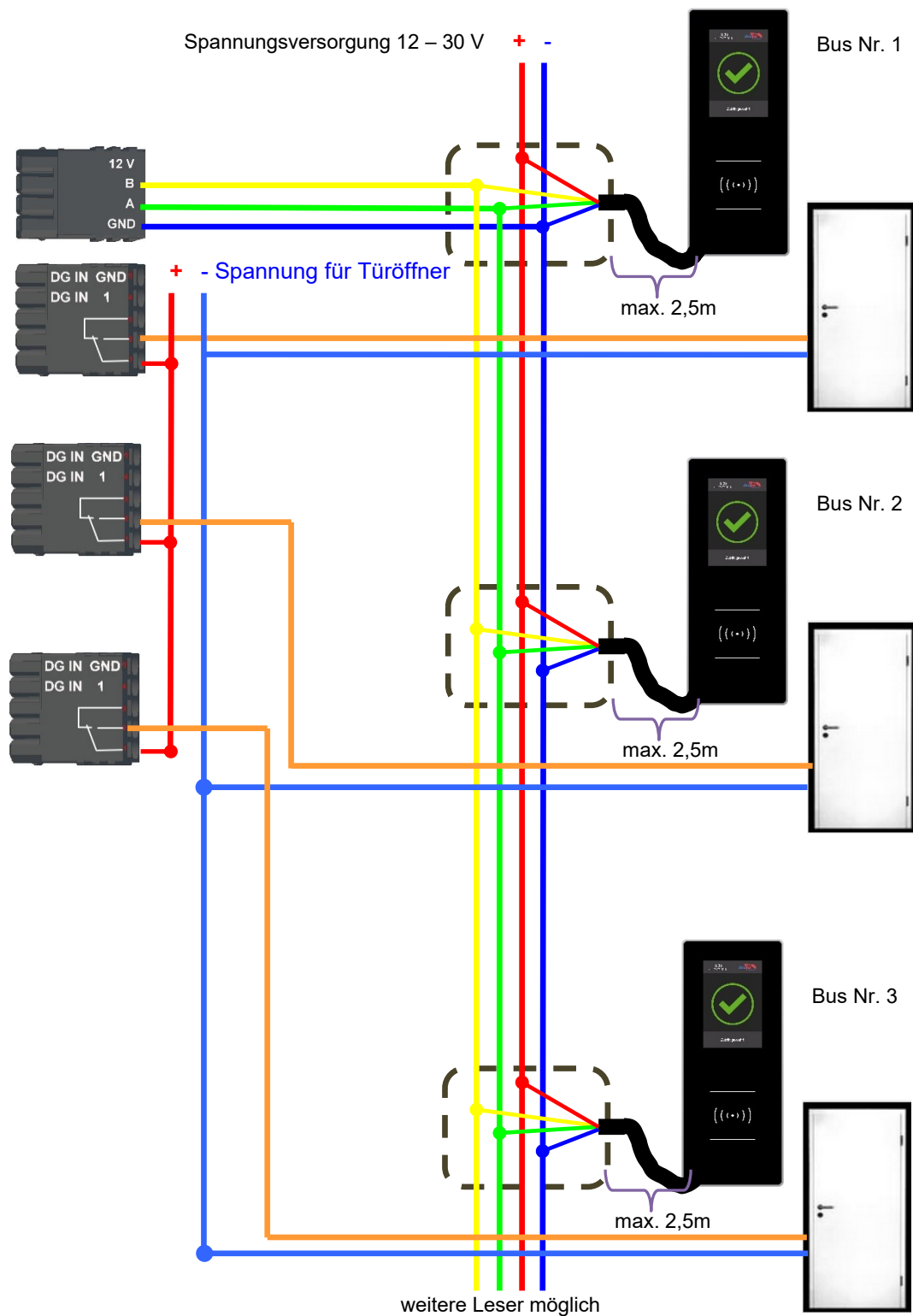
Verkabelungsplan für 3 Türen, 3 Relais in dem EVO 2.8 Pure:



Entsprechende Reader Tabelle, Beispiel:

ID	ZM / Bus-ID	TM (Busadresse)	RefLocation	RefAction	PinGeneral	Beschreibungstext
1	1	010	1	1	0	Leser mit Bus Nr. 1
2	1	020	2	2	0	Leser mit Bus Nr. 2
3	1	030	3	3	0	Leser mit Bus Nr. 3
4	1	320	0	1	0	(Mastergerät)

Verdrahtungsplan für 3 Türen, 3 Relais in dem EVO 2.8 Pure:



5.9.4. Zutrittskontrolle II mit PHG-Modulen

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

EVO 2.8 Pure



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

VOXIO VOXIO T-Z



Unterputz: 81 x 81 x 11 mm (BxHxT)
Aufputz: 81 x 81 x 40 mm (BxHxT)

Der VOXIO kann mit Legic bzw. Mifare eingesetzt werden. Er ist als Unterputz- oder Aufputzvariante mit oder ohne Tastatur erhältlich. Jeder Leser besitzt eine Sabotageerkennung, drei Leuchtfelder zur Visualisierung des Status und einen Buzzer zur akustischen Signalisierung.

RELINO & Relino B



50 x 50 x 43 mm (BxHxT)

Der RELINO (B) Leser kann mit Legic bzw. Mifare eingesetzt werden. Er ist als reine Unterputzvariante erhältlich. Jeder Leser besitzt drei Leuchtfelder zur Visualisierung des Status sowie einen Buzzer zur akustischen Signalisierung.

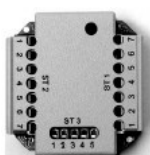
Siedle



100 x 100 x 20 mm (BxHxT)

Der Siedle Leser kann mit 125 kHz, Legic bzw. Mifare eingesetzt werden. Er wird in die Siedle Vario 611 Gehäuseumgebung eingebunden und ist mit und ohne Tastatur erhältlich. Jeder Leser besitzt drei Leuchtfelder zur Visualisierung des Status sowie einen Buzzer zur akustischen Signalisierung.

IO-Box



51 x 48 x 22 mm (LxBxH)

Die IO-Box als Zubehör für den RFID-Wandleser bzw. RELINO Leser besitzt zwei digitale Eingänge und zwei digitale Ausgänge. Als Schnittstelle kommt der I²C-Bus zum Einsatz.

Ab Firmware Version 69806D der PHG Leser wird die Autologinfunktion für Mifare unterstützt. Hierfür können 5 der max. 6 im Setup einstellbaren Keys verwendet werden.



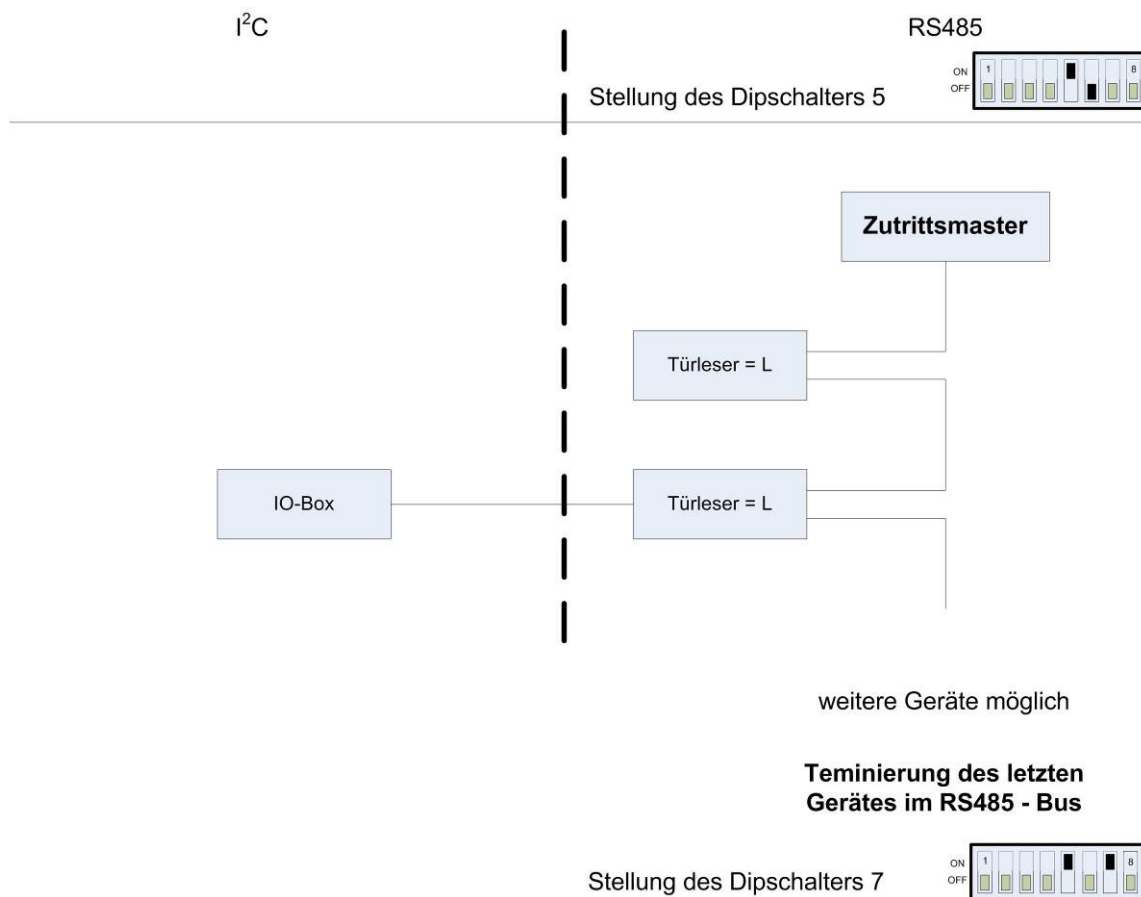
Achtung:

Technische Daten für die PHG Zutrittsmodule finden Sie auf der Datafox DVD oder in unserem Downloadbereich. Beachten Sie bitte den Stromverbrauch der Module und der Spannungsabfall bei großen Kabellängen. Die Verantwortung für die Berechnungen der maximalen Leitungslängen liegt beim Installateur.

5.9.4.1. Anschluss der PHG-Leser

Für den Anschluss der PHG-Module beachten Sie bitte die PHG Dokumentationen auf der Datafox CD unter: <Datafox DVD\MasterIV-Serie u. TimeboyIV\Datafox Geräte\Datafox_Zutritt-Module>

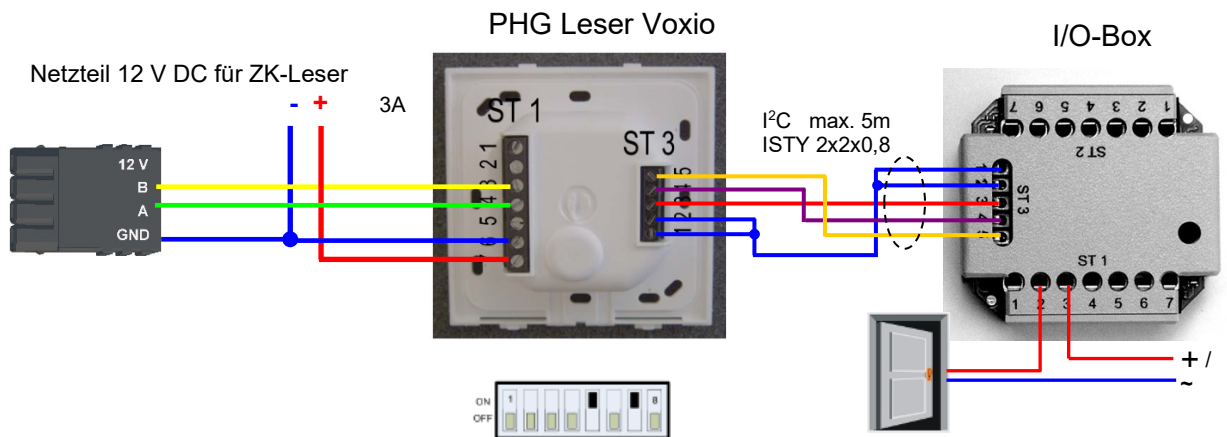
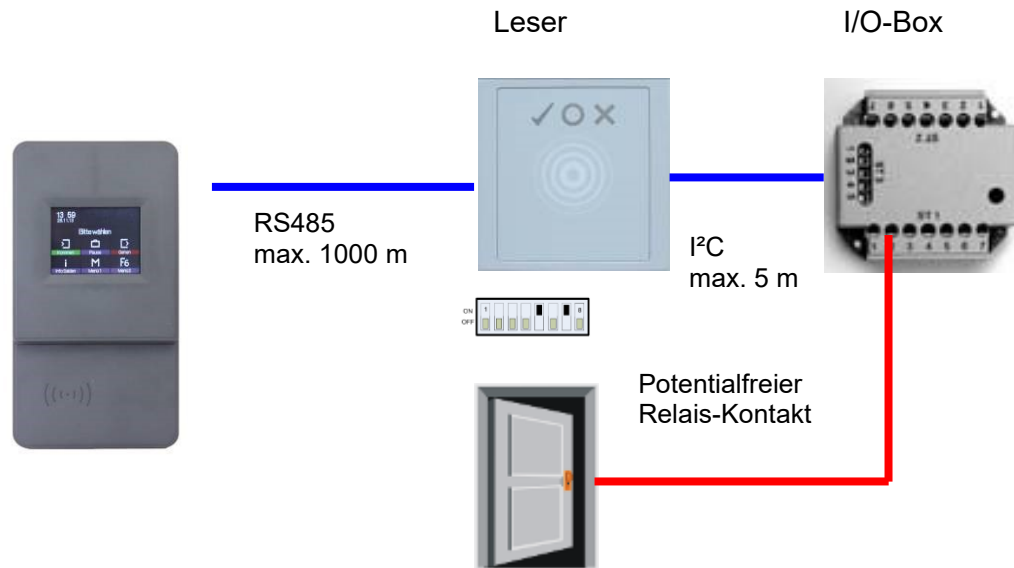
In den PHG Dokumenten zu den einzelnen Modulen, wird die Anschlussbelegung und Konfiguration über die Dip-Schalter beschrieben. Um mit dem EVO 2.8 Pure eine Zutrittskontrolle durchzuführen, muss die Option „Zutritt“ integriert sein. Die folgende Grafik zeigt die Anschlussmöglichkeiten der PHG-Geräte an einen EVO 2.8 Pure für die Zutrittskontrolle.



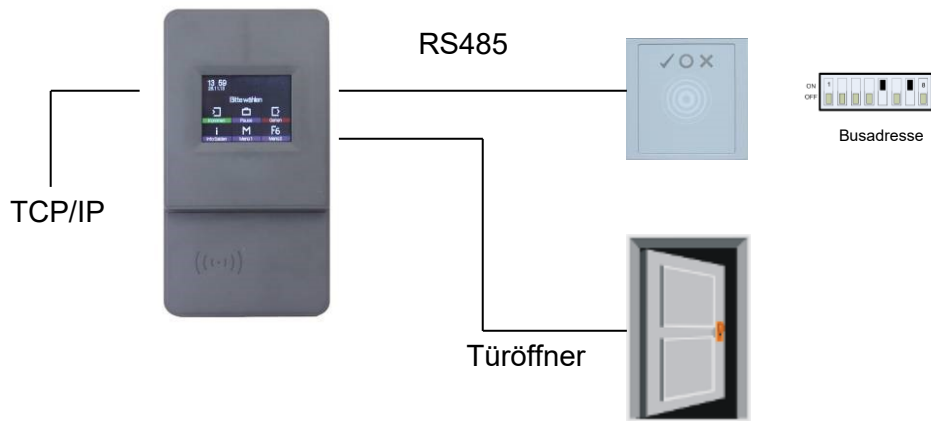
Über die Dip-Schalter 1-4 wird die Bus-Nummer des Moduls eingestellt. Der Dip-Schalter 5 muss immer auf „ON“ gesetzt werden. Die Dip-Schalter 6 und 8 müssen immer auf „OFF“ stehen. Mit dem Dip-Schalter 7 = „ON“ wird am letzten Modul der RS485-Bus terminiert (120 Ω Abschlusswiderstand), sonst immer „OFF“.

Wenn zusätzlich ein Türöffner über ein Relais gesteuert werden soll, muss eine IO-Box zum Einsatz kommen. Mit jeder IO-Box stehen zwei digitale Ausgänge in Form von Relais zur Verfügung.

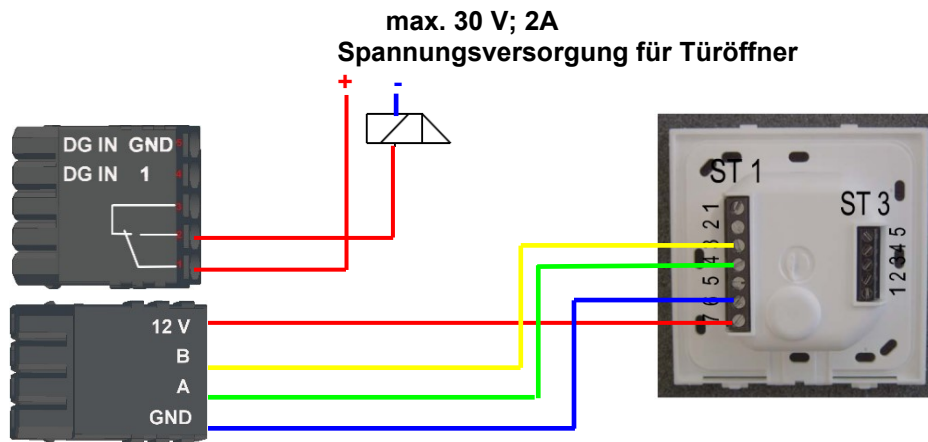
Anschlussbeispiel eine Tür mit I/O-Box:



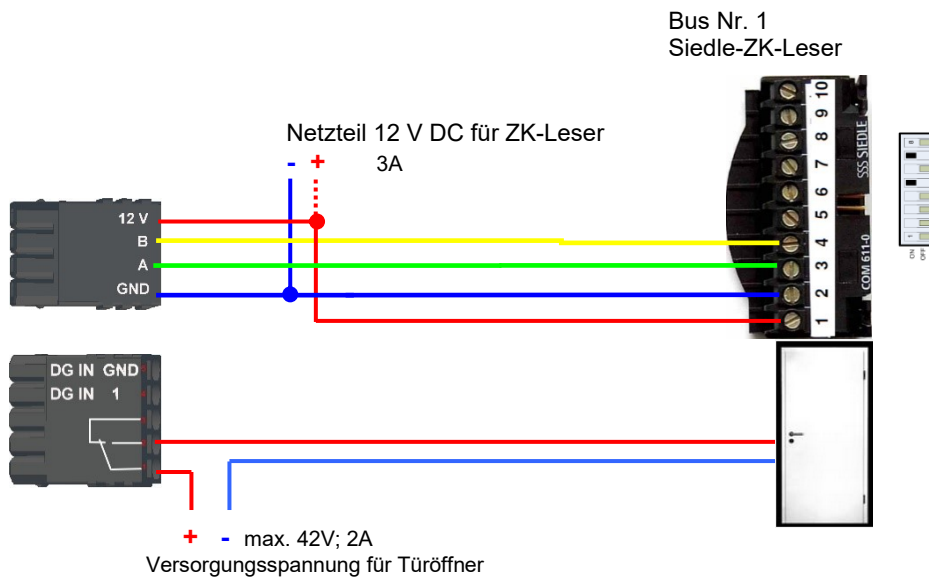
Anschlussbeispiel eine Tür ohne I/O-Box:



Verdrahtungsplan für einen VOXIO-Leser:

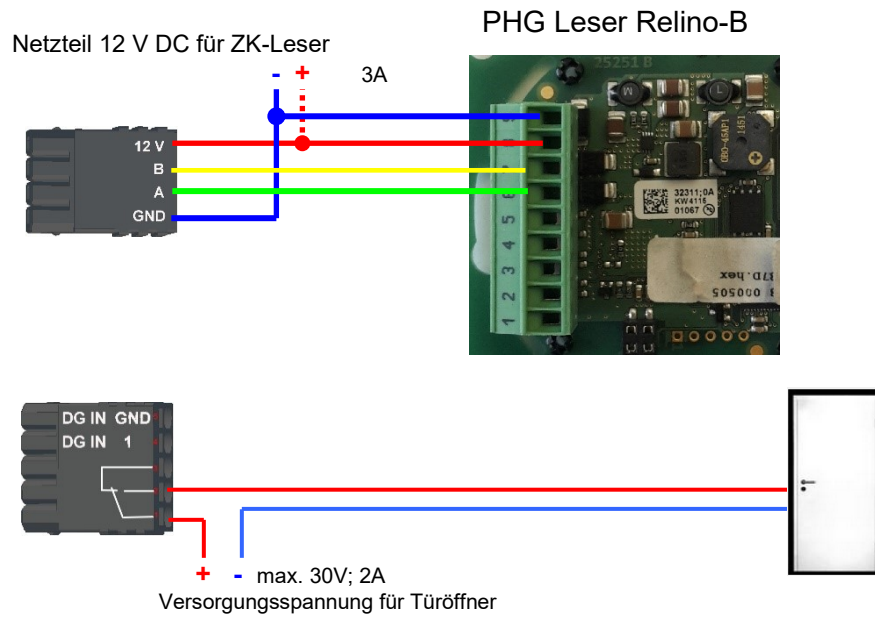


Verdrahtungsplan für einen Siedle-Leser:



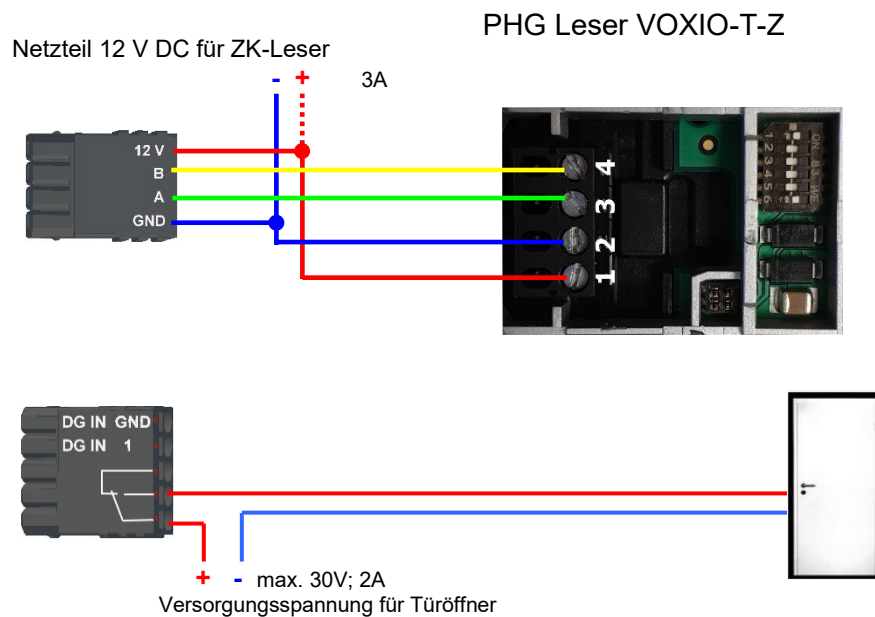
Verdrahtungsplan für einen PHG Relino-B Leser:

! Der Leser Typ wird ab der FW 04.03.09.17 unterstützt.

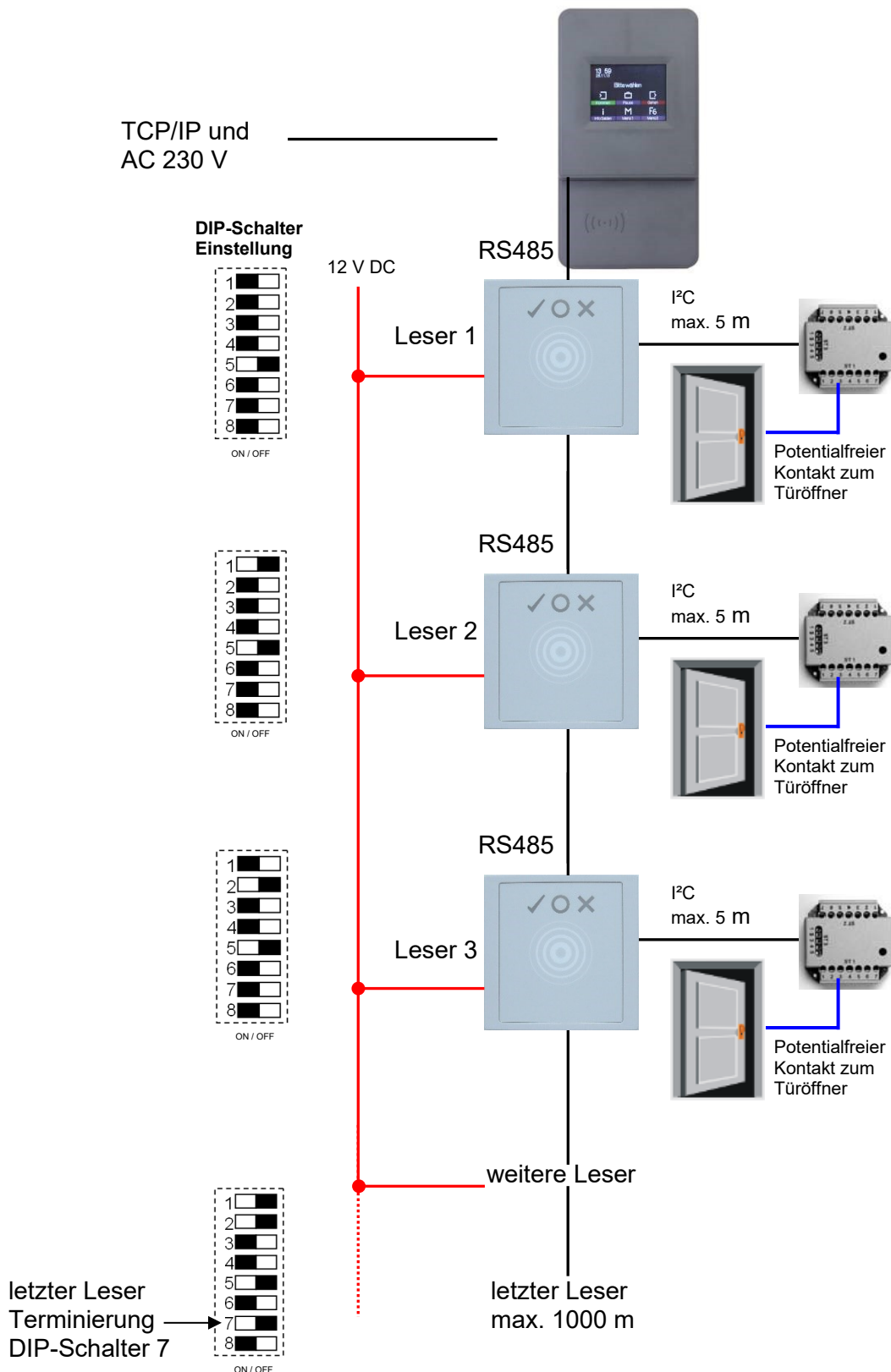


Verdrahtungsplan für einen VOXIO-T-Z Leser:

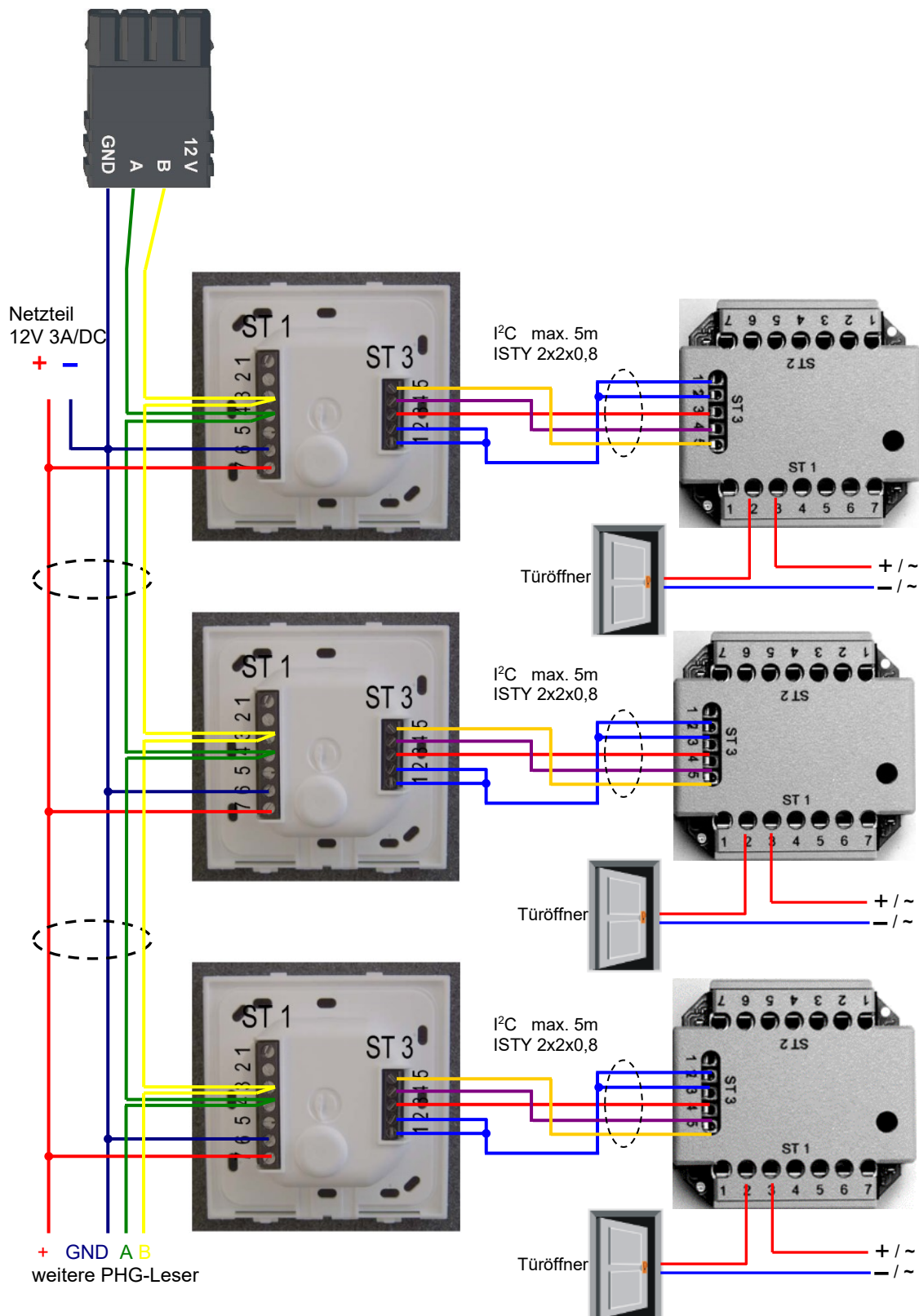
! Der Leser Typ wird ab der FW 04.03.12.xx unterstützt.



Schematischer Aufbau der RS485 Busverkabelung mit 3 ZK-Lesern:



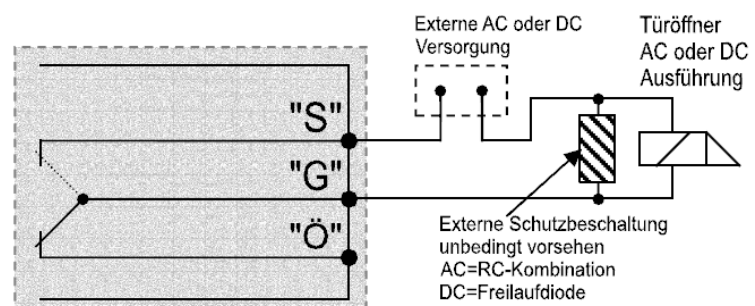
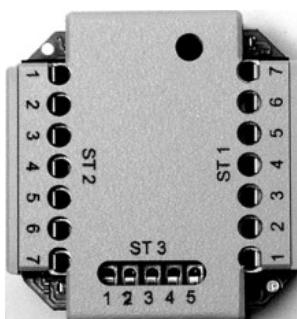
Verdrahtungsplan mehrerer PHG-Leser:



Bei dem Anschluss des Türöffners sollte unbedingt eine Schutzschaltung integriert werden.
Bei DC eine Feilauodiode und AC ein RC-Glied.

Anschlussklemmen der IO-Box:

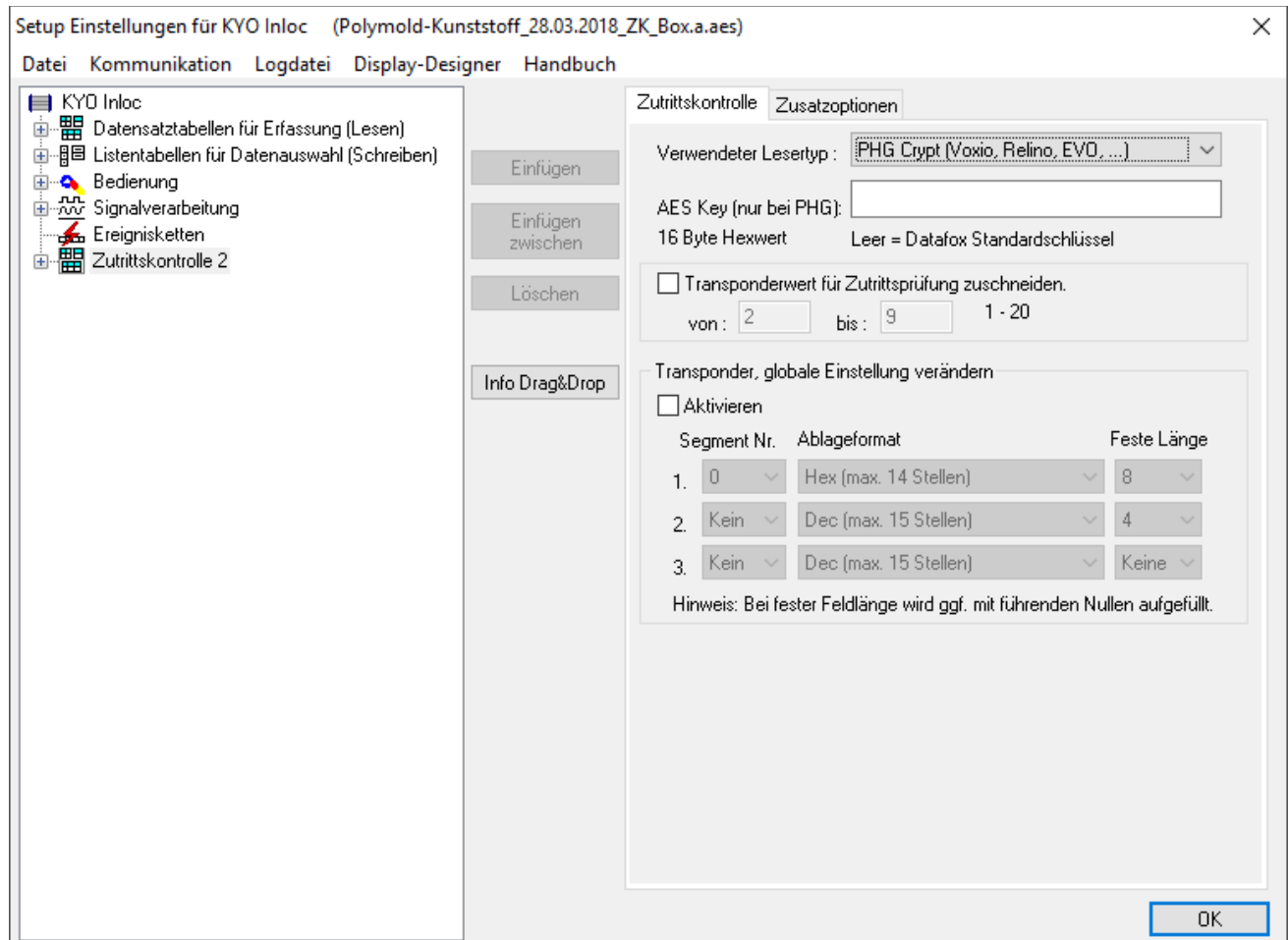
Anschluss (ST1,2,3)	Klemme Nr.	Beschreibung
ST1	1	Relais 1 → „Ö“ Öffner
	2	Relais 1 → „G“ Gemeinsamer
	3	Relais 1 → „S“ Schließer
	4	NC
	5	NC
	6	Eingang 2 Signal
	7	Eingang 2 GND
ST2	1	Relais 2 → „Ö“ Öffner
	2	Relais 2 → „G“ Gemeinsamer
	3	Relais 2 → „S“ Schließer
	4	NC
	5	NC
	6	Eingang 1 Signal
	7	Eingang 1 GND
ST3	1 und 2	GND
	3	U+ 8.....30V
	4	SCL
	5	SDA



ST 1 Schaltbild
 3 = "S"
 2 = "G"
 1 = "Ö"

5.9.4.2. Konfiguration

Die Zutrittsmodule arbeiten mit einer internen Verschlüsselung. Dieser Schlüssel ist bereits im DatafoxStudioIV hinterlegt aber nicht sichtbar.



Ist unter „AES Key (nur bei PHG)“ kein Schlüssel eingetragen, so wird ein Standardschlüssel verwendet.



Achtung:

Ein Wechsel des Schlüssels darf nur in einer fertig eingerichteten Zutrittskontrolle durchgeführt werden. Haben Sie den Schlüssel gewechselt und vergessen, müssen die Module eingeschickt werden. Das Wiederherstellen des Standardschlüssels ist kostenpflichtig.

Alle in der Readertabelle angelegten Türmodule müssen auch tatsächlich im RS485-Netzwerk vorhanden sein um sicherzustellen, dass beim Einspielen eines neuen Setups mit einem anderen Schlüssel dieser auch in allen Modulen gewechselt werden kann. Fehlt ein Türmodul aus der Liste im Bus, erfolgt kein Wechsel des Schlüssels. Es muss wieder das alte Setup mit dem alten Schlüssel übertragen werden, sonst ist nach einem Reboot des Gerätes keine Kommunikation zu den Türmodulen mehr möglich, bis der richtige Schlüssel wieder verwendet wird.

Wird ein defekter Leser gegen einen neuen bisher unbenutzten Leser getauscht, erkennt die Firmware das beim Start automatisch und richtet die Verschlüsselung ein. Der Leser kann auch im laufenden Betrieb gewechselt werden. Die Firmware bindet ihn automatisch ein.

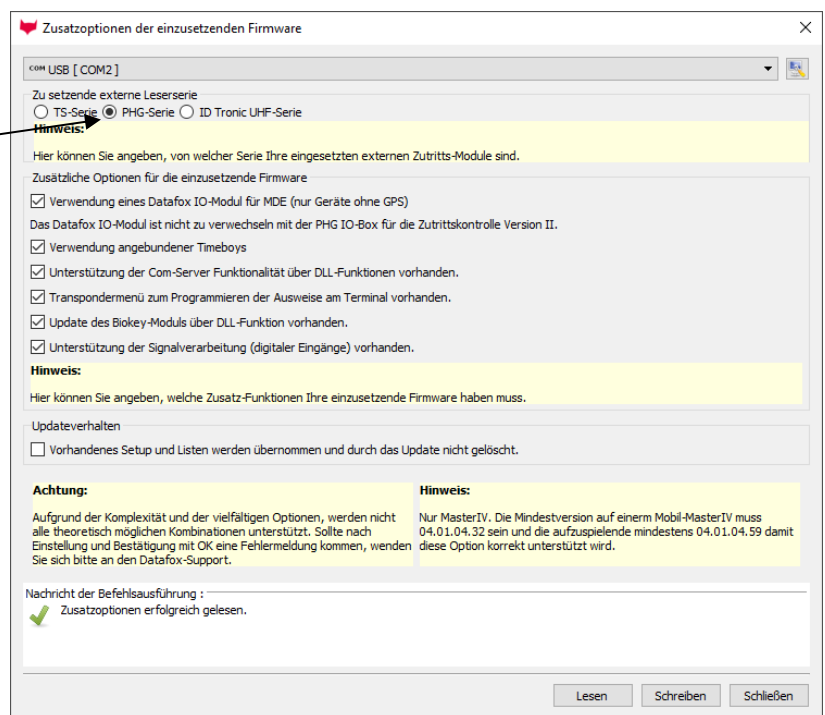
PHG-Leser haben im Gegensatz zu den GIS-Lesern immer 2 digitale Eingänge und einen Sabotagekontakt. Die Firmware betrachtet Eingang 1 und Eingang 2 als normalen Eingang mit der Nummer 1 und 2 den Sabotagekontakt als Nr. 3. Der Sabotagekontakt ist im Leser integriert. Der PHG-Leser verfügt nicht über einen Analog-Schalter-Eingang für die Türüberwachung.

Zusätzlich kann der PHG-Leser mit einer IO-Box erweitert werden. Diese IO-Box besitzt zwei digitale Eingänge und zwei Relaisausgänge. Die IO-Box wird über die gleiche Adresse wie der Leser angesprochen. Die zwei digitalen Eingänge haben die Port-Nummer 4 und 5, die digitalen Ausgänge haben die Port-Nummer 1 und 2. Bei Leitungsunterbrechung oder Sabotage wird Port-Nr. 6 benutzt.

PHG-Module und Firmware:

Wenn Sie die PHG-Module nutzen möchten, so muss dies in den Zusatzoptionen eingestellt werden.

Nach dem Umstellen auf die Zutrittsleser der Serie PHG muss die Firmware neu übertragen werden. Das Gerät sucht sich dann die entsprechende Firmware aus der .dfz-Datei aus.



Alle Konfigurationen wie Tabellen usw. sind wie bei den Zutrittslesern der TS-Serie zu erstellen. Einzige Ausnahme:

Die IO-Box wird nicht extra in der Readertabelle angegeben. Somit entfallen die Angaben über die Module, welche als Stich über den I²C-Bus angeschlossen sind.

Entsprechende Readertabelle:

ID	ZM	TM	RefLocation	RefAction	PinGeneral	Beschreibungstext
1	1	320	0	1	0	Mastergerät
2	1	010	1	1	0	Leser an RS485 (PHG)
3	4	044	4	4	0	IO-Box an I ² C-Bus
4	1	020	2	2	0	Leser an RS485 (LTM)
5	4	024	2	2	0	IO-Box an I ² C-Bus

5.9.5. Zutrittskontrolle II mit TS-Lesern

Folgende Hardware steht für den Aufbau einer Zutrittskontrolle mit TS TMR33-Modulen zur Verfügung. Entsprechend der Hardwareanforderung der einzelnen Geräte können diese in verschiedenen Varianten miteinander kombiniert werden.

EVO 2.8 Pure



Das Datafox Gerät unterstützt die Türöffnung von bis zu 8 Türen.

Türmodul (TS TMR33-TM)

72 x 72 x 40 mm



Das Türmodul (**TM**) enthält Relais, um einen Türöffner anzusteuern. Das Türmodul wird als reine elektronische Baugruppe angeboten. Es kann in eine Unterputzdose oder in einer Aufputzdose (links dargestellt) mit Sabotagekontakt montiert werden.

Leser (TS TMR33-L)

80 x 80 x 25 mm



Der Leser (**L**)(ohne Relais) kann auch separat bezogen werden, um ihn direkt an einen PC oder an eine andere Zutrittssteuerung anzuschließen. Es werden ein Anschlussplan und eine Beschreibung der Befehle zur Ansteuerung mitgeliefert.

Kombimodul = Leser + Türöffnerfunktion (TS TMR33-LTM)

80 x 80 x 25 mm



Das Kombimodul (**LTM**) (Transponderleser und Relais) kann auch separat bezogen werden, um es direkt an einen PC oder an eine andere Zutrittssteuerung anzuschließen. Es werden ein Anschlussplan und eine Beschreibung der Befehle zur Ansteuerung mitgeliefert.



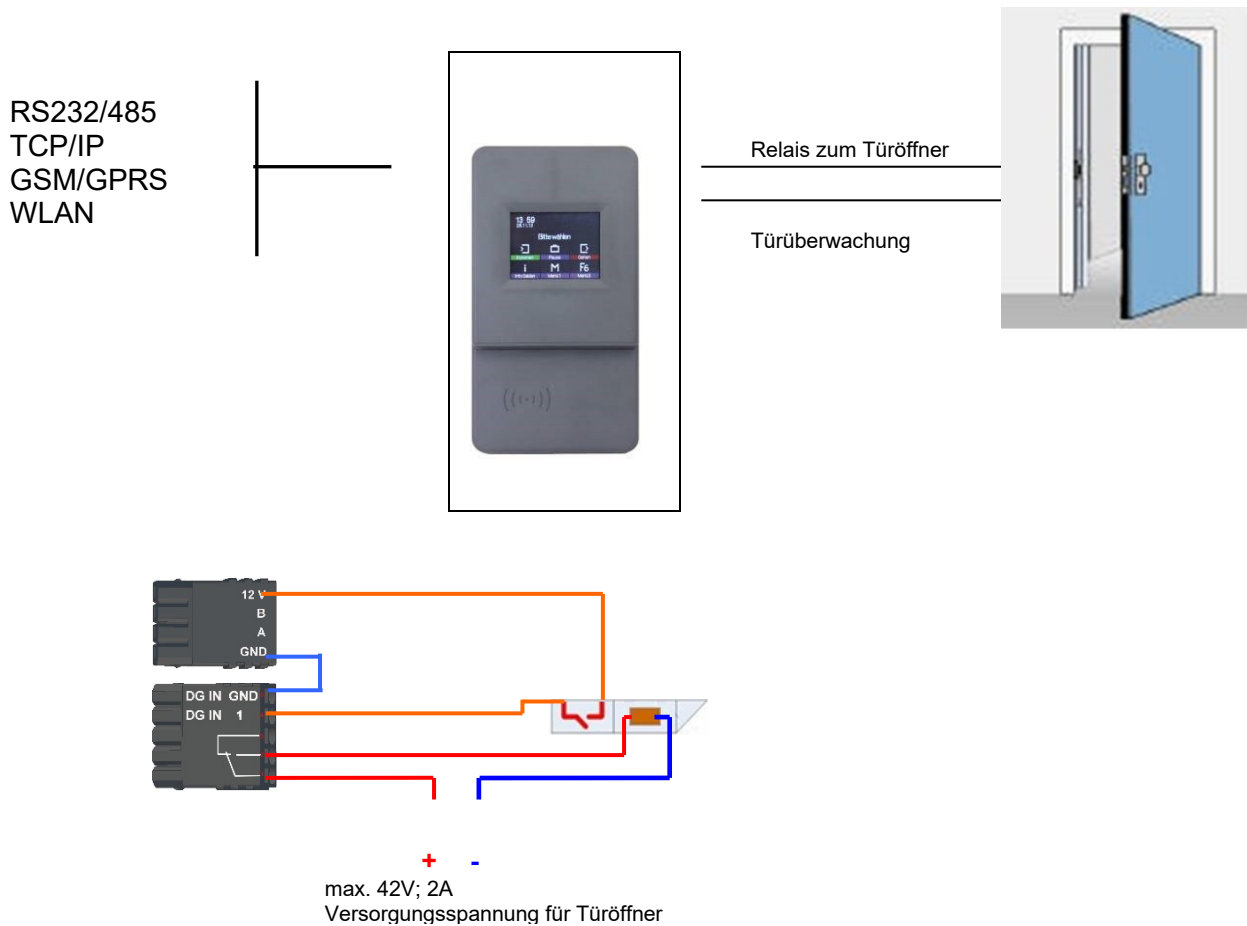
Hinweis:

Die einzelnen Module werden an einen Bus angeschlossen. Hierbei legt der Dippschalter 5 fest, ob diese über RS232 oder RS485 kommunizieren sollen.

5.9.5.1. Aufbau und Installationsvarianten

Eine Tür ohne separaten Leser

Der EVO 2.8 Pure ist gleichzeitig Zutrittsleser, Zutritts-Master und Türöffner. Diese Lösung sollte nur im geschützten Bereich eingesetzt werden, damit das Türöffner-Relais nicht manipuliert werden kann.



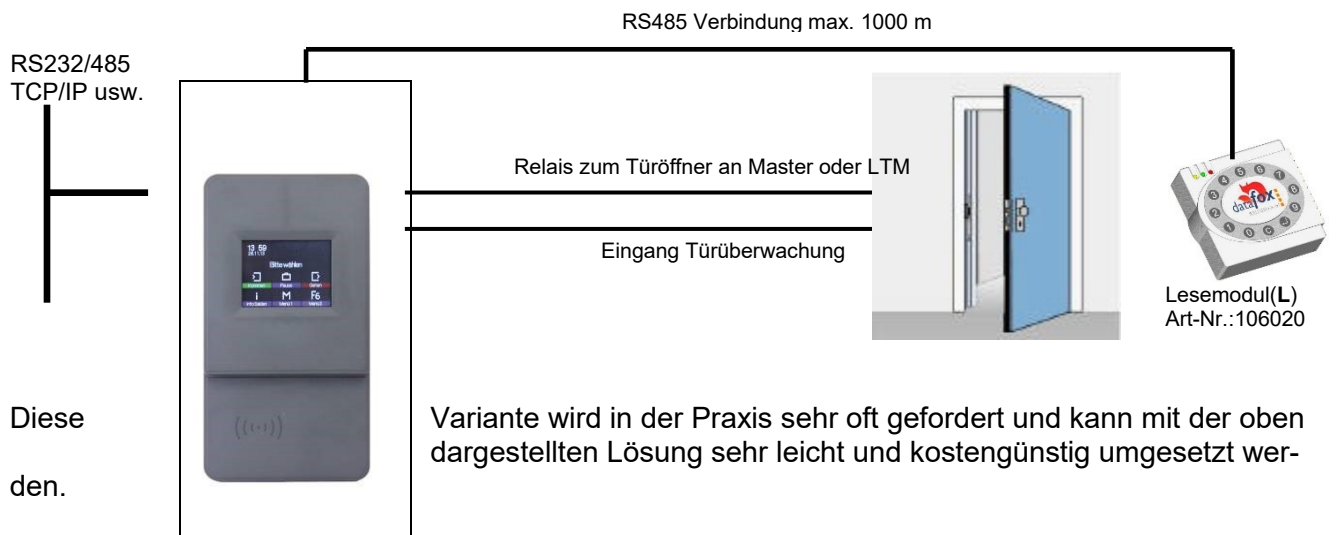
Achtung:

Die Installation und der Anschluss der TMR33-Module darf nur von geschultem Fachpersonal durchgeführt werden. Dabei ist eine Verpolung der Anschlussklemmen zu vermeiden.

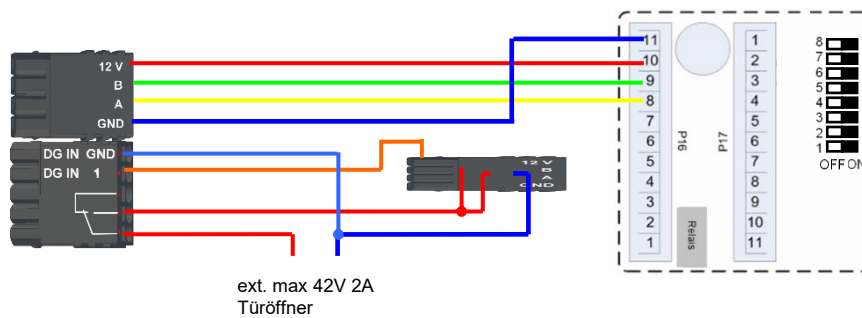
Eine Tür mit abgesetztem Leser

Der EVO 2.8 Pure wird im geschützten Bereich im Gebäude installiert, der Leser außen. Das Terminal ist gleichzeitig Zutritts-Master und Türöffner. Das Türöffner-Relais befindet sich im EVO 2.8 Pure und damit im geschützten Bereich. Die am Leser erfasste Zugangskennung wird auf den EVO 2.8 Pure übertragen und ausgewertet. Ist der Zutritt erlaubt, wird über das Relais im Master/EVO 2.8 Pure die Tür geöffnet.

Übersichtsplan:



Verdrahtungsplan:



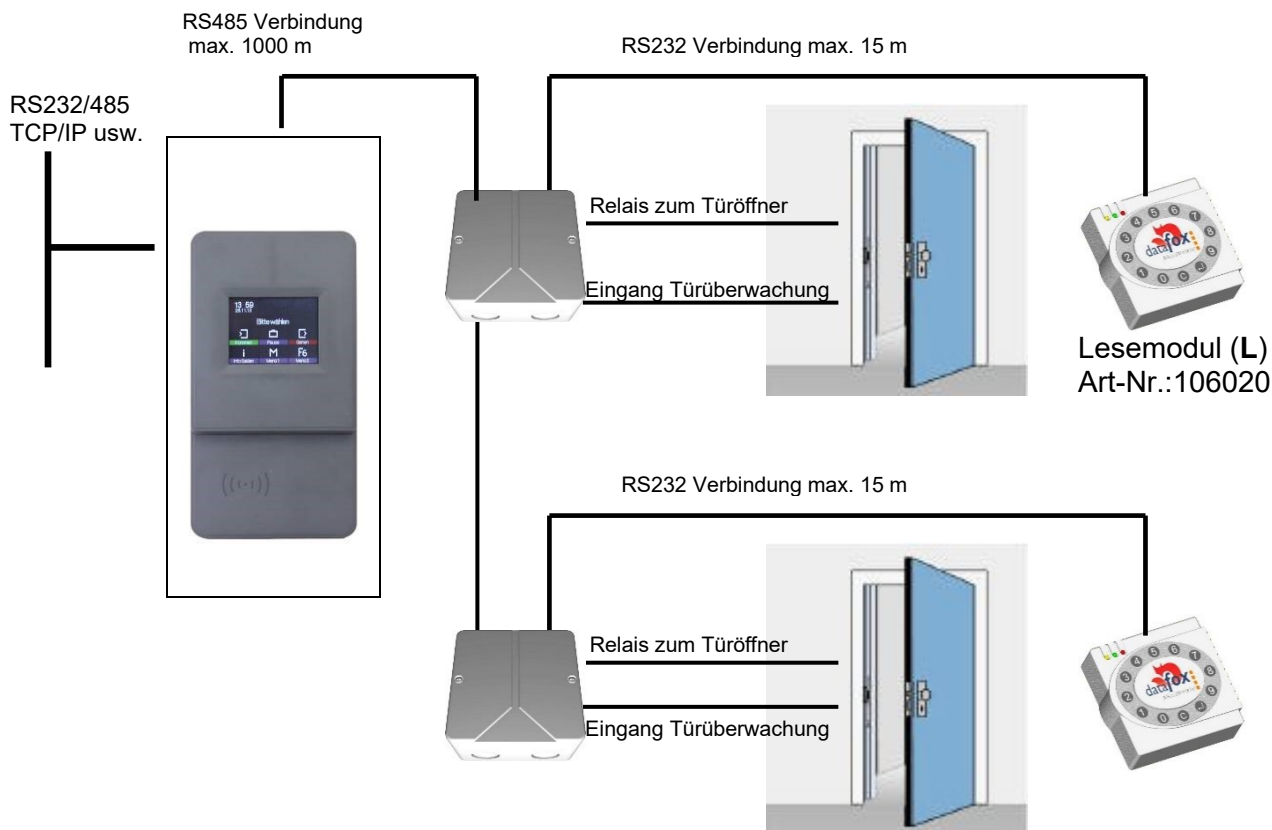
Entsprechende Reader Tabelle

ID	ZM	TM	RefLocation	RefAction	PinGeneral	Beschreibungstext
1	1	320	0	1	0	Mastergerät
2	1	010	1	1	0	Leser an RS485 (L)

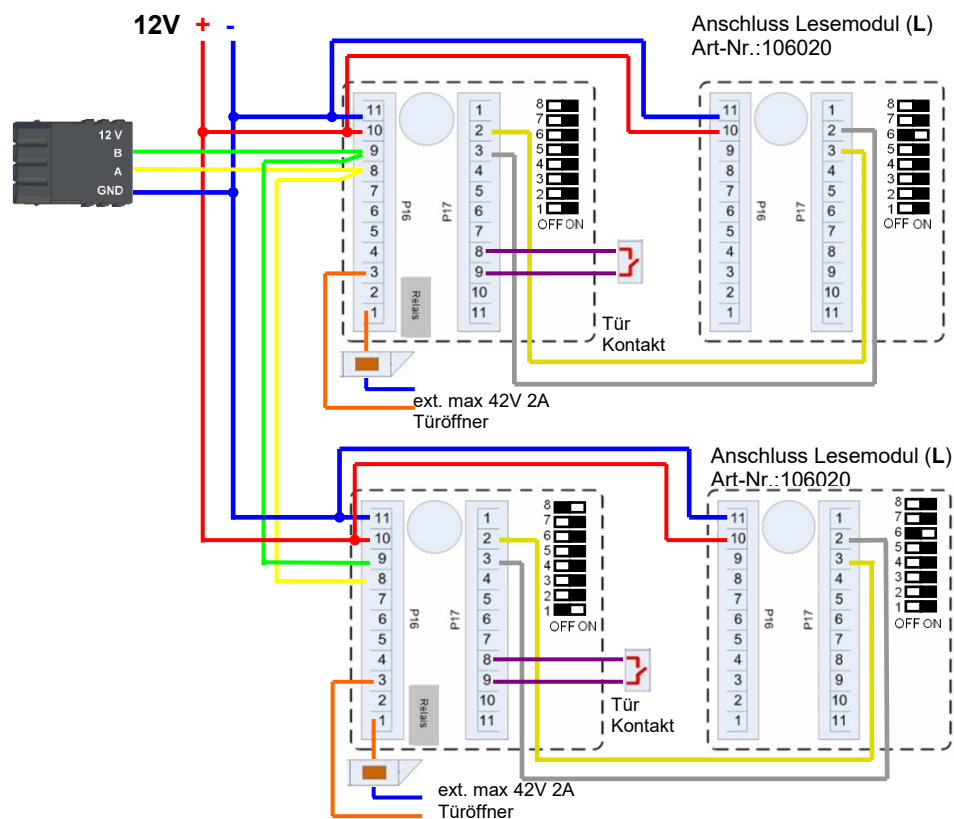
Mehrere externe Türen über RS485 - Bus

Hier muss das Türmodul zum Einsatz kommen, damit sich das Türöffner-Relais im geschützten Bereich befindet.

Übersichtsplan:



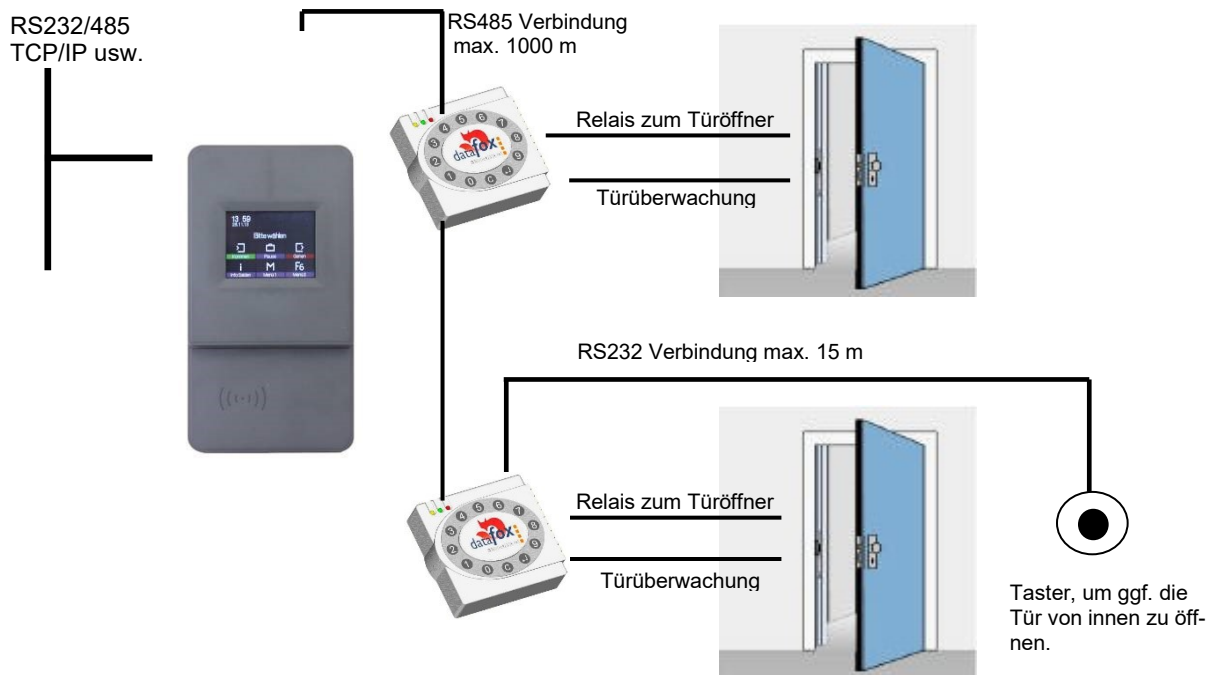
Verdrahtungsplan:



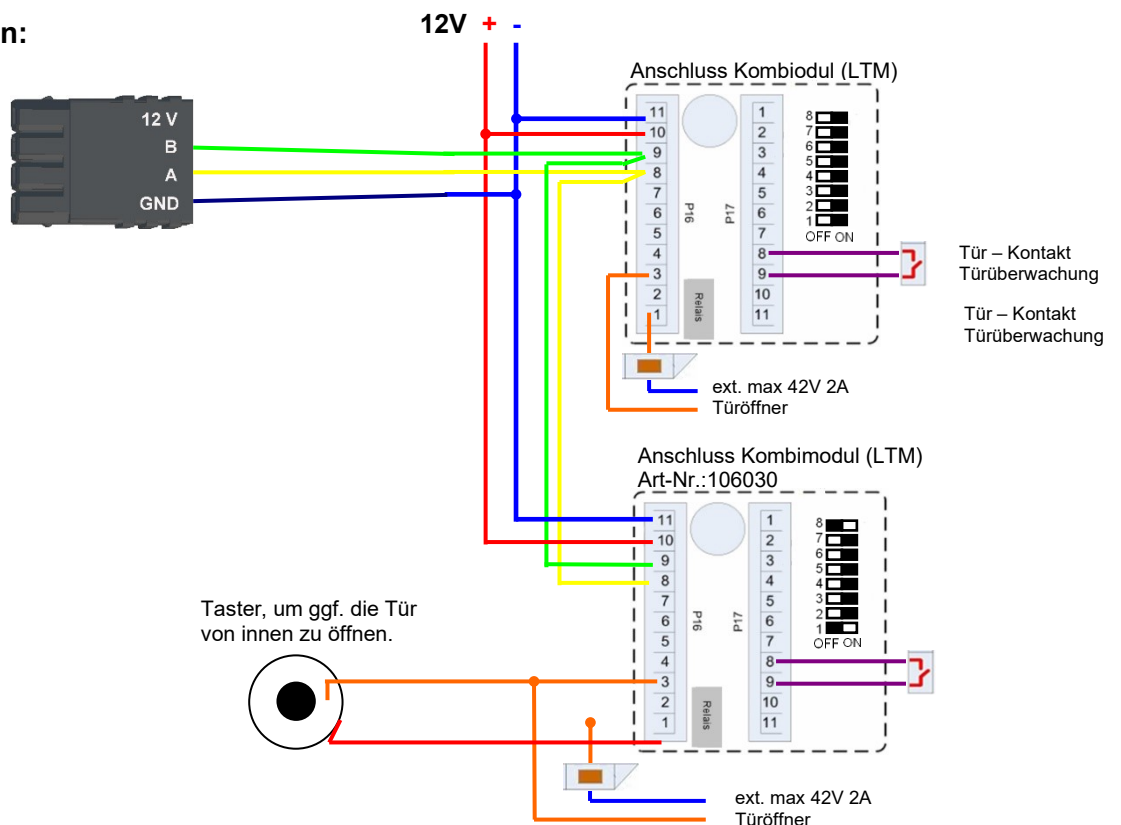
Mehrere interne Türen über RS485 - Bus

Hier kommt das kombinierte Leser + Tür-Modul zum Einsatz (**LTM**). Das Türöffnerrelais ist im Kombimodul enthalten. Achtung! Dieser Aufbau darf nicht im Außenbereich eingesetzt werden, da sich das Relais dann nicht im geschützten Bereich befindet.

Übersichtsplan:



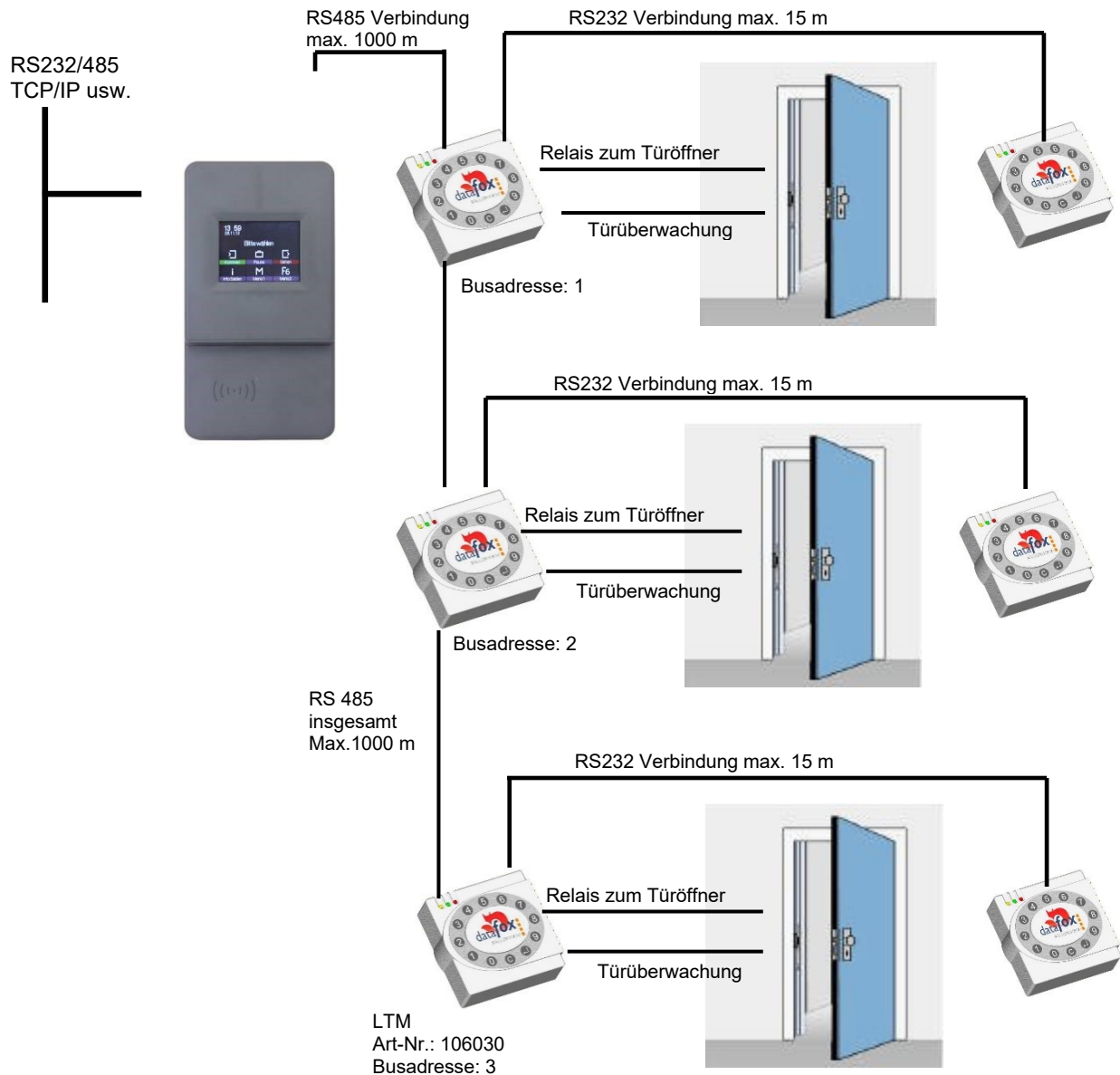
Verdrahtungsplan:



Schleusenfunktion mit RS485 - Bus

Hier kommen das kombinierte Leser+Tür-Modul und der Leser zum Einsatz.

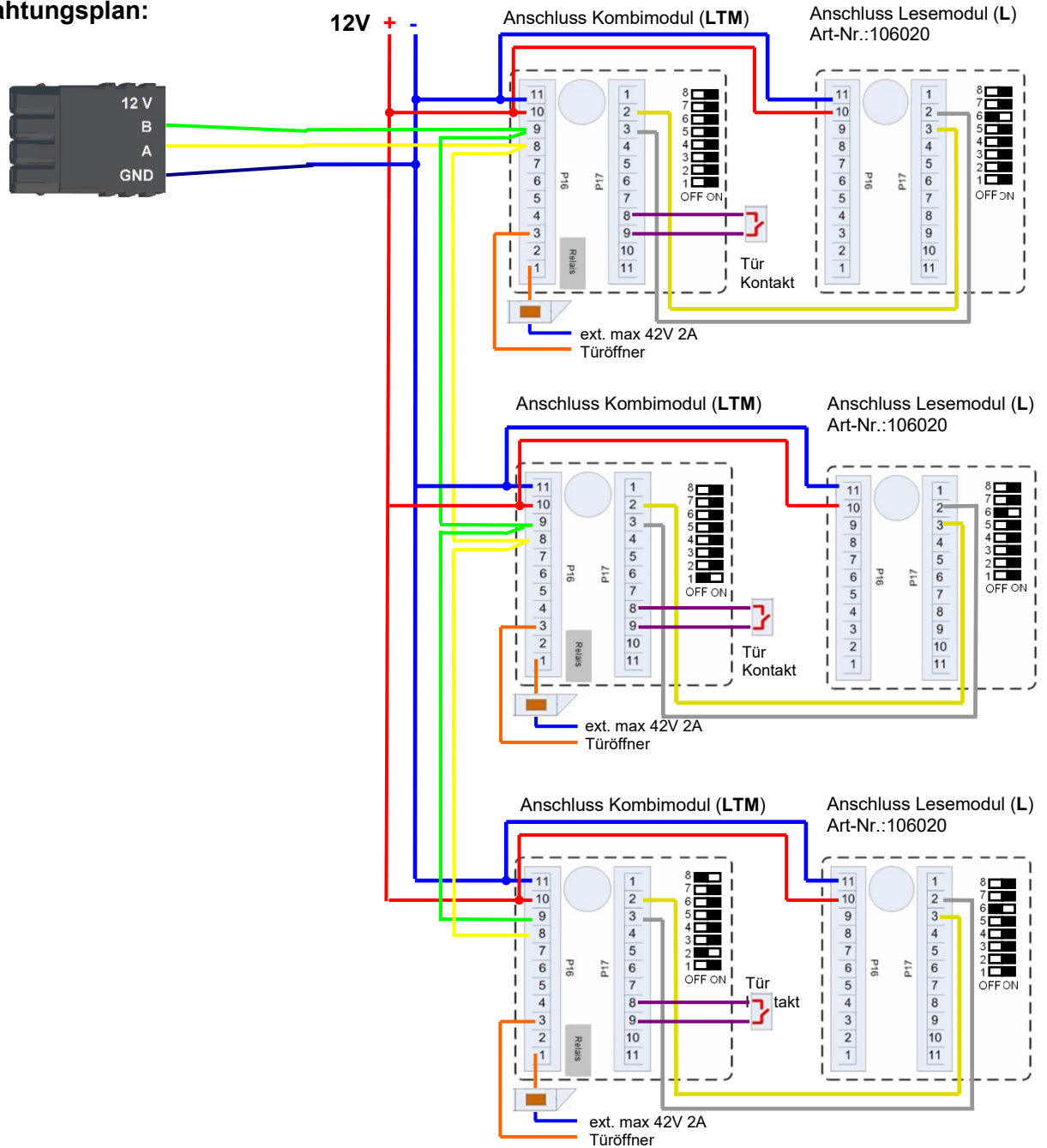
Übersichtsplan:



Entsprechende Readertabelle:

ID	ZM	TM	RefLocation	RefAction	PinGeneral	Beschreibungstext
1	1	320	0	1	0	Mastergerät
2	1	010	1	1	0	Leser und Türmodul an RS485 (LTM)
3	1	011	1	1	0	Leser über RS232 (L)
4	1	020	2	2	0	Leser und Türmodul an RS485 (LTM)
5	1	021	2	2	0	Leser über RS232 (L)
6	1	030	3	3	0	Leser und Türmodul an RS485 (LTM)
7	1	031	3	3	0	Leser über RS232 (L)

Verdrahtungsplan:



Hinweis:

Anschluss für Stromversorgung über Netzteil oder Klingeltrafo. Beachten Sie die Hinweise zur Berechnung des Leitungsquerschnittes bzw. der Leitungslänge.

Bei Außentüren ist der Türöffner im geschützten Bereich zu montieren.

Bei geschlossenem Türkontakt werden ca. 15 mA bei 12 V verbraucht = 0,18 Watt. Das entspricht einem Verbrauch von ca. 1,6 kWh/Jahr.



5.9.5.2. Anschluss der TS-Leser

Um mit dem EVO 2.8 Pure eine Zutrittskontrolle durchzuführen, muss die Option „Zutritt“ integriert sein (Datafox Artikel-Nr. 105201). Die folgende Grafik zeigt die Anschlussmöglichkeiten der TMR33-Geräte an einen EVO 2.8 Pure für die Zutrittskontrolle. Je nach verwendeter Schnittstelle (RS232 oder RS485) müssen die TMR33-Geräte eingestellt werden.

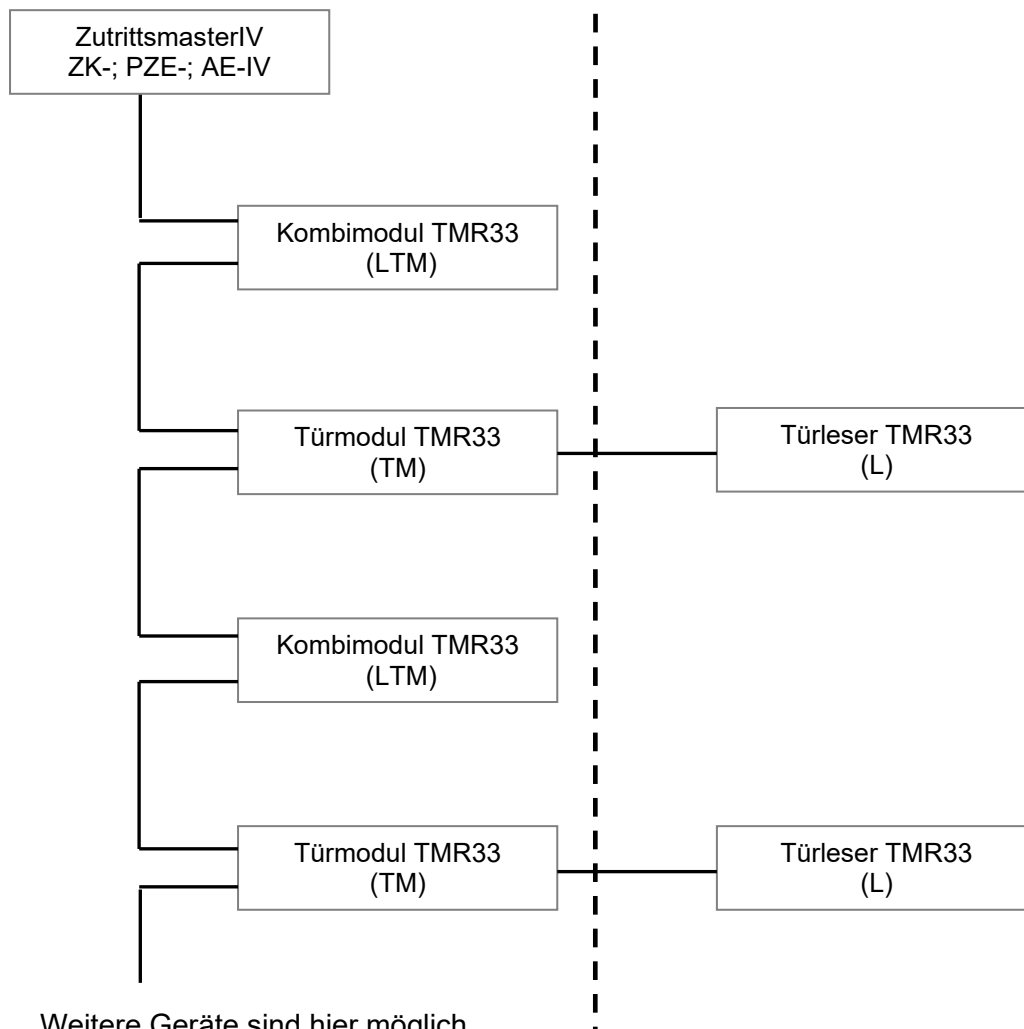
RS 485

RS 232

Stellung des Dipschalters 6



Stellung des Dipschalters 6



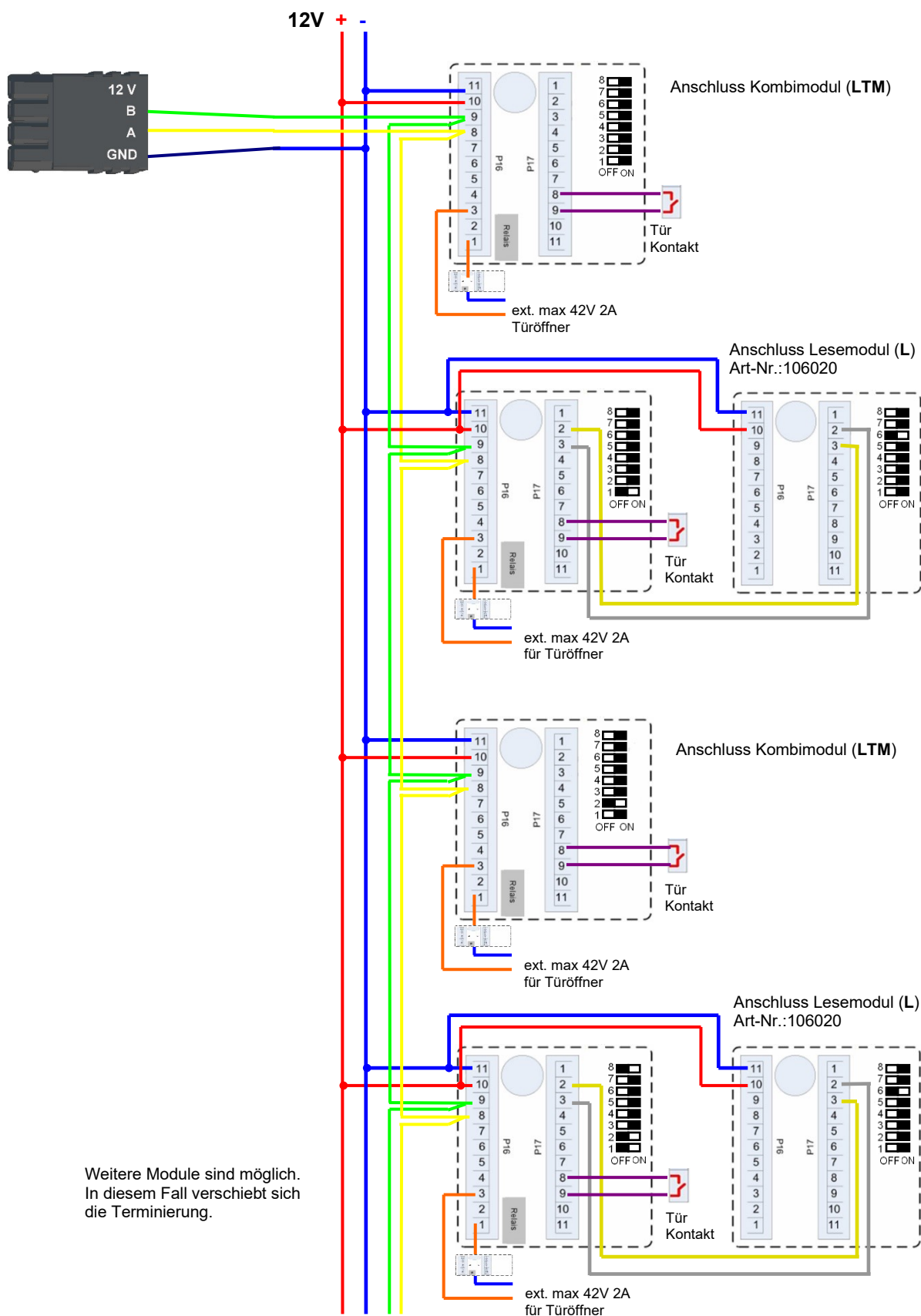
Weitere Geräte sind hier möglich.
PZE-MasterIV bis 8 Module
ZK-MasterIV bis 16 Module

Dipschalter 8 am letzten Modul für die Terminierung:



Die Dip-Schalter 1-5 dienen der Bus-Konfiguration. Mit ihnen wird die Bus-Nr. des Gerätes eingestellt. Der Dip-Schalter 1 in der Position „ON“ und 2-5 in der Position „OFF“ entspricht der Bus-Nr „1“. Der Dip-Schalter 1 und 2 in der Position „ON“ und 3-5 in der Position „OFF“ entspricht der Bus-Nr „3“.

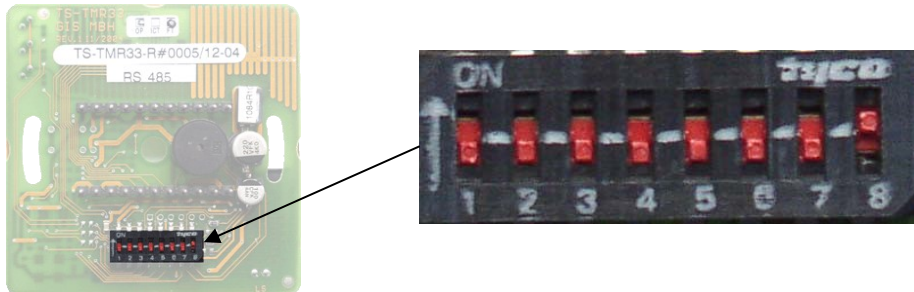
Verdrahtungsplan:



Weitere Module sind möglich.
In diesem Fall verschiebt sich
die Terminierung.

Einstellung der DIP-Schalter TS-TMR33

Die Adressierung der Busteilnehmer erfolgt über die *DIP-Schalter 1-5* (Bereich 0-31). Der *DIP-Schalter 6* dient der Umschaltung von RS232 auf RS485 Kommunikation (bei Türmodulen kann bei RS232-Kommunikation kein externer Leser mehr angeschlossen werden). Der *DIP-Schalter 7* ist unbenutzt, und muss immer auf *OFF* stehen. Mit dem *DIP-Schalter 8* wird die *Terminierung* des RS485 Bus ein/ausgeschaltet, dieser Schalter muss immer am letzten Modul des RS485-Busses eingeschaltet (ON) sein.



DIP-Schalter	Bedeutung
1	Busnummer (Bit 0)
2	Busnummer (Bit 1)
3	Busnummer (Bit 2)
4	Busnummer (Bit 3)
5	Busnummer (Bit 4)
6	Umschaltung RS232 auf RS485 (0=RS485, 1=RS232)
7	immer auf OFF
8	Terminierung des RS485 Bus (0=Terminierung aus, 1=Terminierung ein)

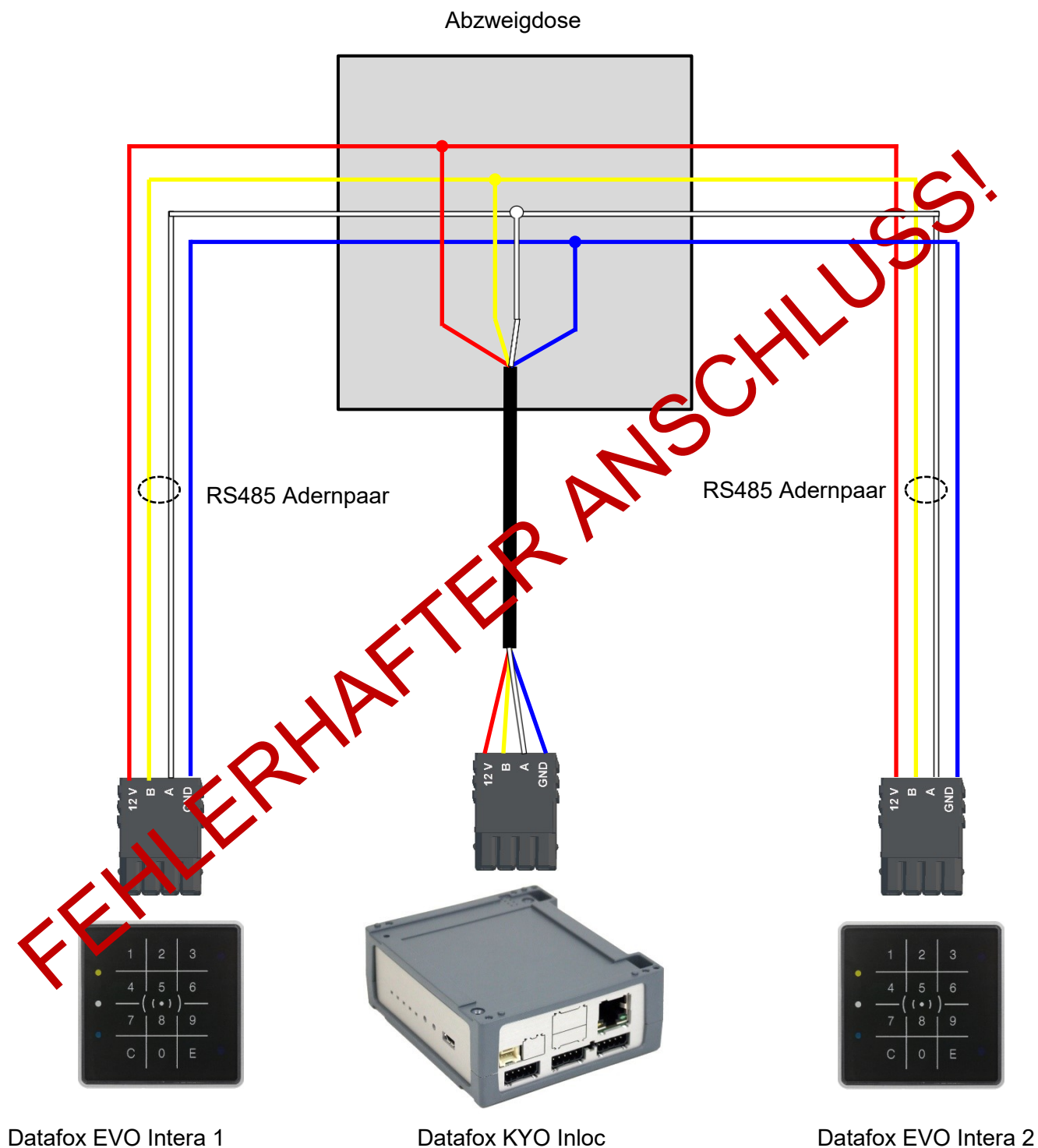
Busadressen setzen:

Adresse	Bit 0	Bit 1	Bit 2	Bit 3	Dippschalter
0	0	0	0	0	
1	1	0	0	0	
2	0	1	0	0	
3	1	1	0	0	
4	0	0	1	0	
5	1	0	1	0	
6	0	1	1	0	
7	1	1	1	0	
8	0	0	0	1	
9	1	0	0	1	
Usw.					

5.9.6. Hinweise für den Elektriker zur Installation der Zutrittskontrolle

5.9.6.1. Busverkabelung Sternförmig

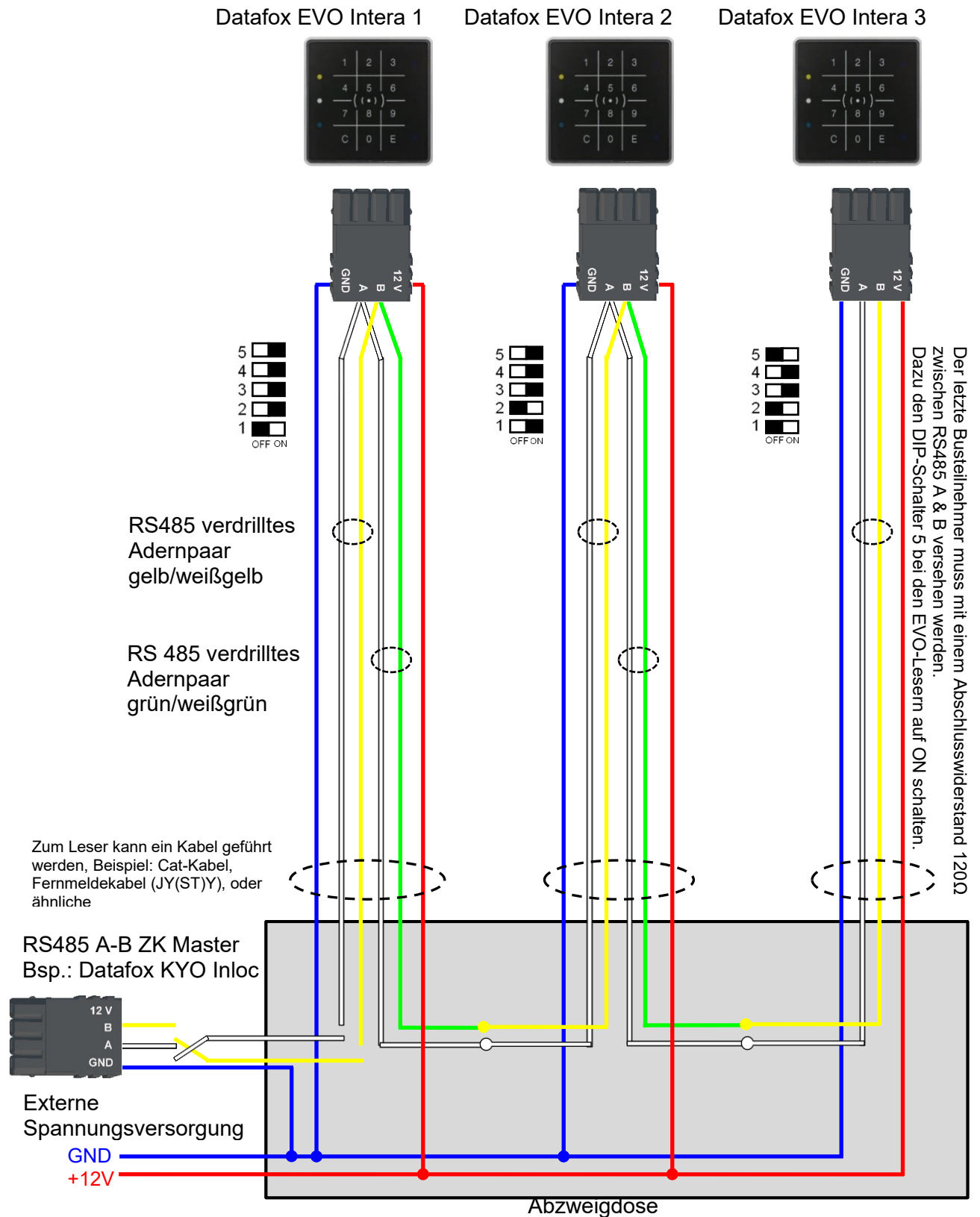
**! Falscher sternförmiger Anschluss des RS485-Busses.
RS485 Adernpaare dürfen nicht parallel geschaltet werden.**



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.



5.9.7. Berechnungsvorschrift für die Spannungsversorgung der ZK-Module

Beim Einsatz von Zutrittslesern, ist vor der Errichtung eines RS485-Netzwerkes für die Zutrittskontrolle der notwendige Leitungsquerschnitt bzw. die maximale mögliche Leitungslänge zu berechnen. Die Mindestspannung darf für den jeweiligen Leser darf dabei nicht unterschritten werden.

Max. Stromverbrauch und maximale und minimale Spannung der einzelnen Module:

TS-TMR33-TR	56,5 mA	16 V max. 8 V min. DC
TS-TMR33-TM	156,0 mA	16 V max. 8 V min. DC
TS-TMR33-TMR	180,0 mA	16 V max. 8 V min. DC
EVO Intera	250,0 mA	30 V max. 9 V min. DC
EVO Intera II	250,0 mA	30 V max. 9 V min. DC
EVO Agera	400,0 mA	30 V max. 9 V min. DC
PHG-ZK-Leser	250,0 mA	24 V max. 9 V min. DC

Daraus ergibt sich ein max. zulässiger Stromverbrauch pro Datafox Gerätenetzteil von (8 x 180,0 mA + 8 x 56,5 mA) 1,9 Ampere. Um das zu gewährleisten, kann entweder für eine geplante Leitungslänge der notwendige Querschnitt oder zu einem gegebenen Leitungsquerschnitt die max. zulässige Leitungslänge berechnet werden.



Achtung:

In jedem Fall ist eine Berechnung vor Errichtung und Inbetriebnahme eines ZK-Netzwerkes durch geschultes Fachpersonal durchzuführen.

Der Leitungsquerschnitt berechnet sich wie folgt:

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

Q	=	Leitungsquerschnitt in mm ²
I	=	Stromstärke
l	=	Leitungslänge in m
k	=	Leitfähigkeit für Kupfer 56 $\frac{m}{\Omega \cdot mm^2}$

Für 12 V Spannungsversorgung gilt:

U_v = Spannungsabfall max. 4 V TMR33

U_v = Spannungsabfall max. 3 V PHG und EVO Intera

U_v errechnet sich aus Versorgungsspannung minus Mindestspannung für den Leser.

Daraus abgeleitet die Formel zur Berechnung der max. Leitungslänge bei gegebenem Leitungsquerschnitt:

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

5.9.7.1. Leitungslängen für PHG und EVO Intera

Verkabelung und Leitungsführung:

Als Busleitungen können Leitungen mit einem Ader-Durchmesser von 0,6 oder 0,8 mm verwendet werden.

Folgende Leitungstypen eignen sich z.B. als Busleitung:

- J-Y(ST)Y (Fernmeldeleitung),
- YR (Klingelmantelleitung),
- A-2Y(L)2Y (Fernmeldekabel)
- CAT (Netzwerkkabel Installation)

Die maximale Gesamtleitungslänge **BUS RS485** A und B Ader beträgt 1000 m. Hier sind unbedingt ein verdrehtes Aderpaar für die Datenleitung A und B zu verwenden.

Leitungslängen für die Spannungsversorgung der Zutrittsleser. Am Beispiel EVO Intera.

Spannungsversorgung 1 Leser des **Zutritt-Controllers und dessen Netzteil 12V / POE:**

- **0,6** mm Durchmesser: **200** m,
- **0,8** mm Durchmesser: **350** m.

Spannungsversorgung 1 Leser über **separates Netzteil 12V:**

- **0,6** mm Durchmesser: **250** m,
- **0,8** mm Durchmesser: **400** m.

Spannungsversorgung 2 Leser über **separates Netzteil 12V:**

- **0,6** mm Durchmesser: **125** m,
- **0,8** mm Durchmesser: **200** m.

Spannungsversorgung 3 Leser über **separates Netzteil 12V:**

- **0,6** mm Durchmesser: **65** m,
- **0,8** mm Durchmesser: **130** m.

usw.

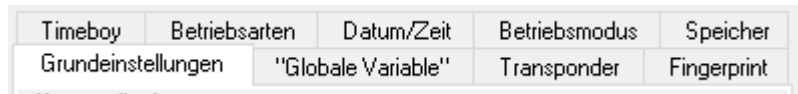
Spannungsversorgung 1 Leser über **separates Netzteil 24V:**

- **0,6** mm Durchmesser: **500** m,
- **0,8** mm Durchmesser: **800** m.

5.9.8. Onlinefunktionen der Zutrittskontrolle

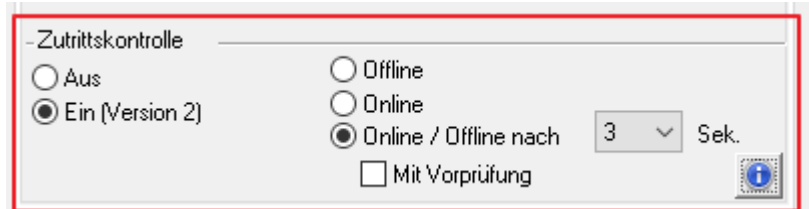
Sie haben die Möglichkeit, bei der Steuerung der Zutrittskontrolle (ZK) alle Entscheidungen und Aktionen der ZK in Ihre Software zu legen. Somit können Sie in Echtzeit auf alle Anforderungen an einer ZK reagieren.

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.



5.9.8.1. 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`

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

access=010	Busadresse, auf der die Aktion durchgeführt werden soll
module=010	Busadresse, auf der die Aktion durchgeführt werden soll
master=1	Bus-Strang auf dem geschaltet werden soll
mask=5	Rote LED + Buzzer
type=1	einschalten
duration=2	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
access= oder module= 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.
master =	1-3 1 2	Id für den RS485 Bus ZK, Beschreibt den ZK-Bus-Strang. RS485 Bus ID 1 RS485 Bus ID 2 usw. „ master “ muss gemeinsam mit „ module “ eingesetzt werden und ersetzt damit „ access “
mask	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 1 Relais angesprochen. Bei gesetztem Bit, wird das 2 Relais angesprochen. Bei gesetztem Bit, wird das 3 Relais angesprochen. Bei gesetztem Bit, wird das 4 Relais angesprochen. Bei gesetztem Bit, wird das 5 Relais angesprochen. Bei gesetztem Bit, wird das 6 Relais angesprochen. Unbenutzt. Bitte immer auf 0 setzen.
type	0 1 2 3	Aus Ein Wechsel (600ms an, 600ms aus) 3 mal einschalten für 500ms
duration	Sekunden / 0	Ist eine Zeitdauer und nur bei type = 1 gültig. Bedeutung: 0 = ständig ein, 1 - 40 = Sekunden ein.



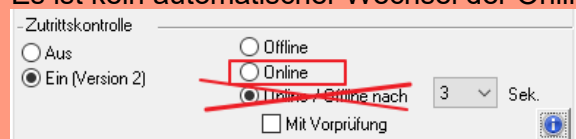
Hinweis:

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.

5.9.8.2. 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

5.9.9. Funktionserweiterung für die Zutrittskontrolle 2

5.9.9.1. 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:

5.9.9.2. Beispiele

Beispiel Werkstatt

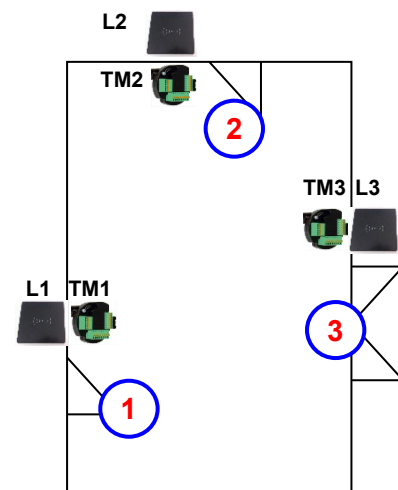
Der Hausmeister kommt am Morgen um 7.00 Uhr und nutzt dabei einen Eingang **1**.

> 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.

5.9.9.3. 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
Buchungen am Leser 1								
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.
Buchungen am Leser 2								
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.
Buchungen am Tor (Leser 3)								
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	

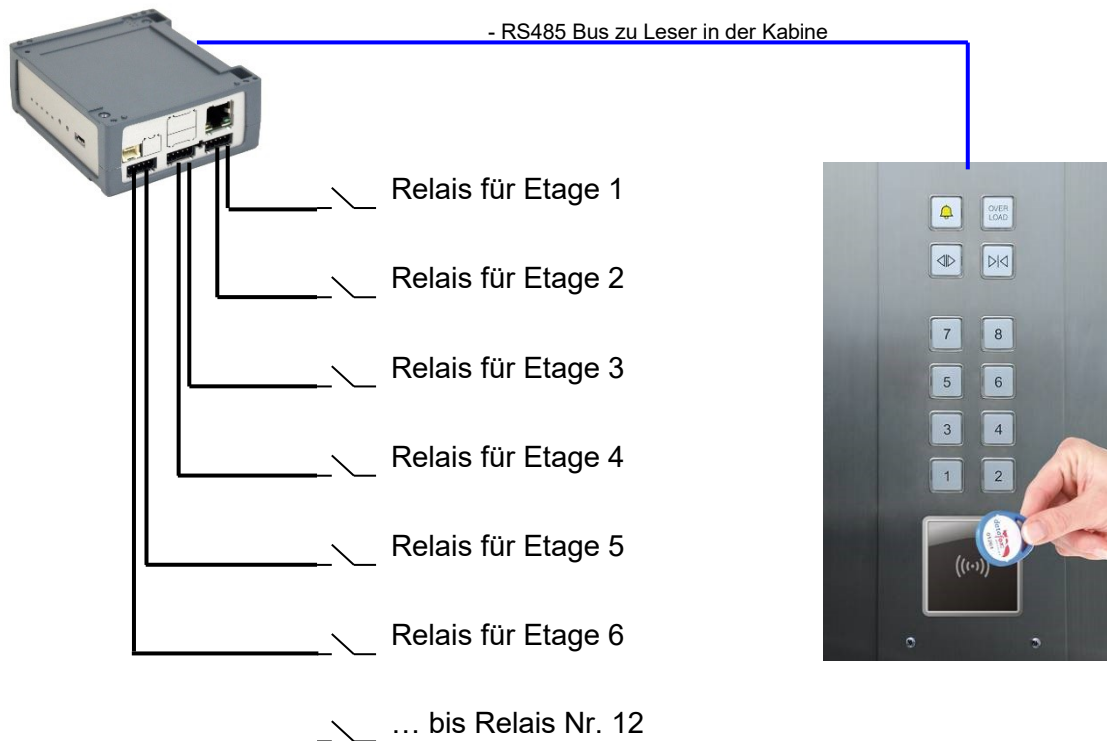
Tabelle *Identification*

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

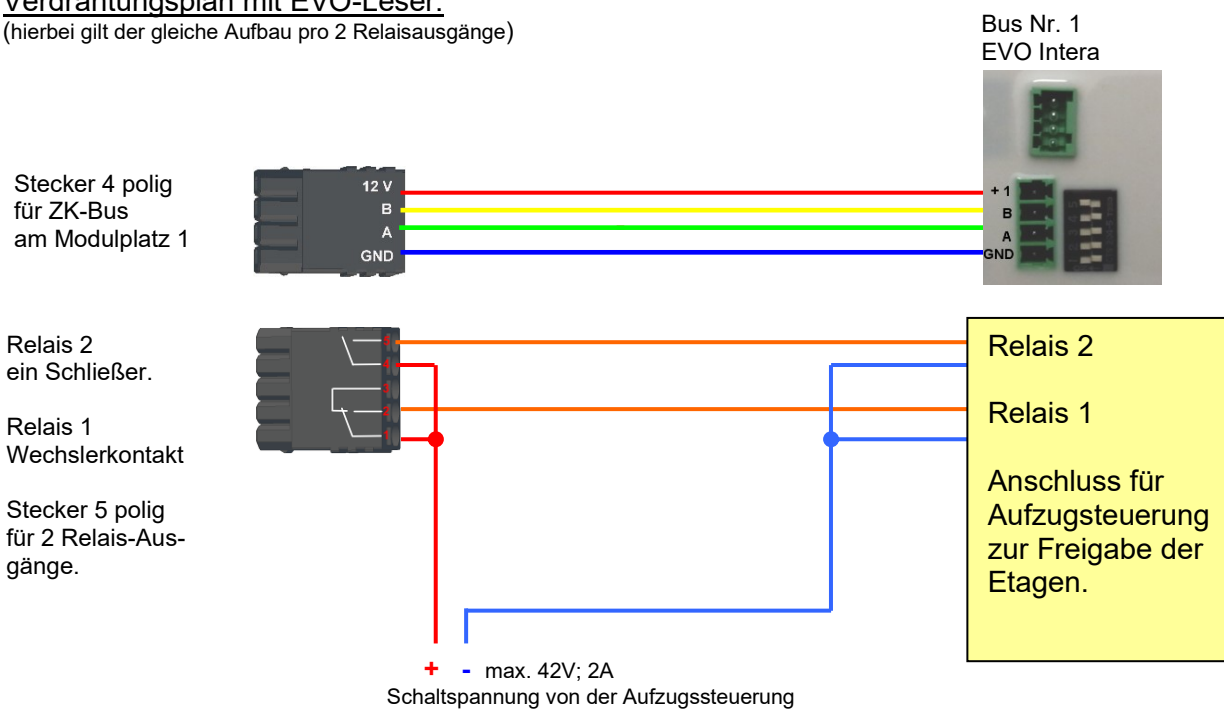
Ziel ist es, das die jeweiligen Mieter nur in ihre Etage fahren dürfen. Hält der Mieter seinen Transponder vor, so wird der Taster am Bedienfeld im Fahrstuhl für die Etage, in der der Mieter wohnt, für 20 Sekunden freigegeben.

In der Aufzugskabine ist ein Transponderleser angebracht und die Steuerung (EVO 2.8 Pure) 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

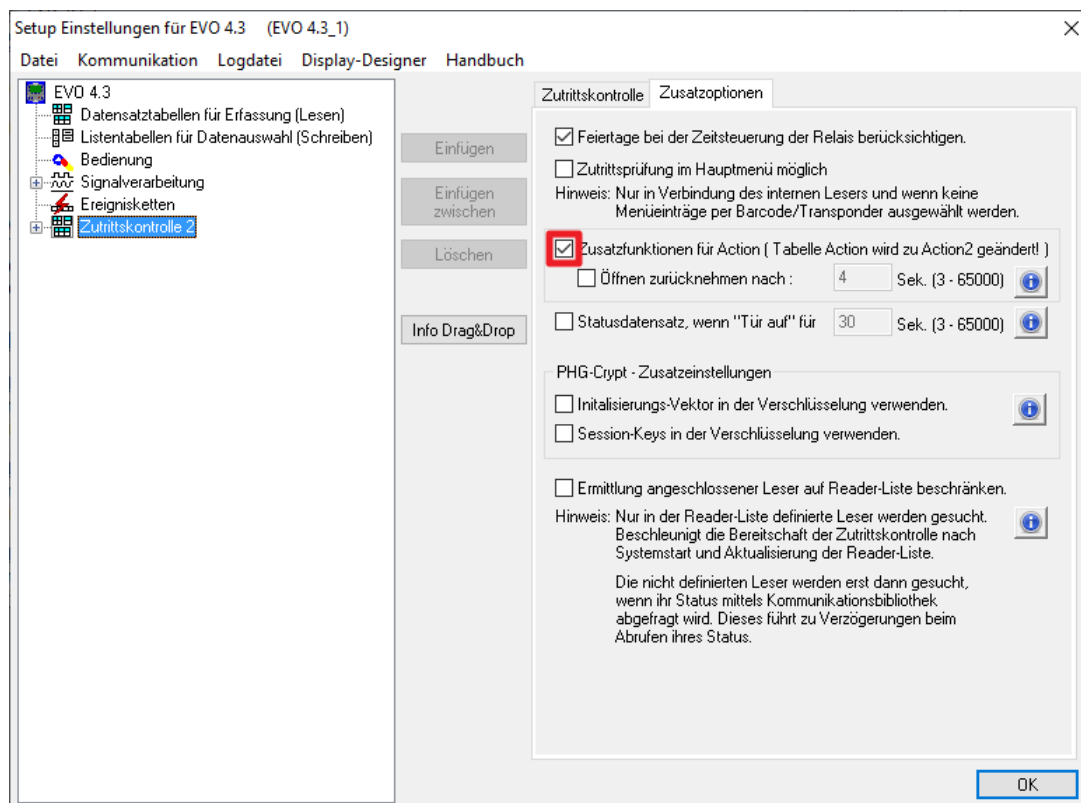
ID	Group	Pin	Menace	ActiveStart	ActiveEnd	Active	Beschreibung
1111	10	0	0	2005-01-01	2099-12-31	1	Mieter Wohnung 1. Etage
2222	20	0	0	2005-01-01	2099-12-31	1	Mieter Wohnung 2. Etage
3333	30	0	0	2005-01-01	2099-12-31	1	Mieter Wohnung 3. Etage
4444	40	0	0	2005-01-01	2099-12-31	1	Mieter Wohnung 4. Etage
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

5.9.9.4. 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) ! Nicht mit Zeitangaben in RefTimeRelais vermischen!
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. ! Die Angabe erfolgt hier in Sekunden! 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. ! Aktionen die hier ausgeführt werden, dürfen nicht mit Zutrittsaktionen gemischt werden!

! 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.

5.9.9.5. 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 Antipassback: 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.

5.9.9.6. 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

5.9.10. 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.

5.9.10.1. 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.

5.9.10.2. 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.

5.9.10.3. 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.

5.9.10.4. 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.

5.9.10.5. 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 5.9.10.3, 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. 5.9.10.3, 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

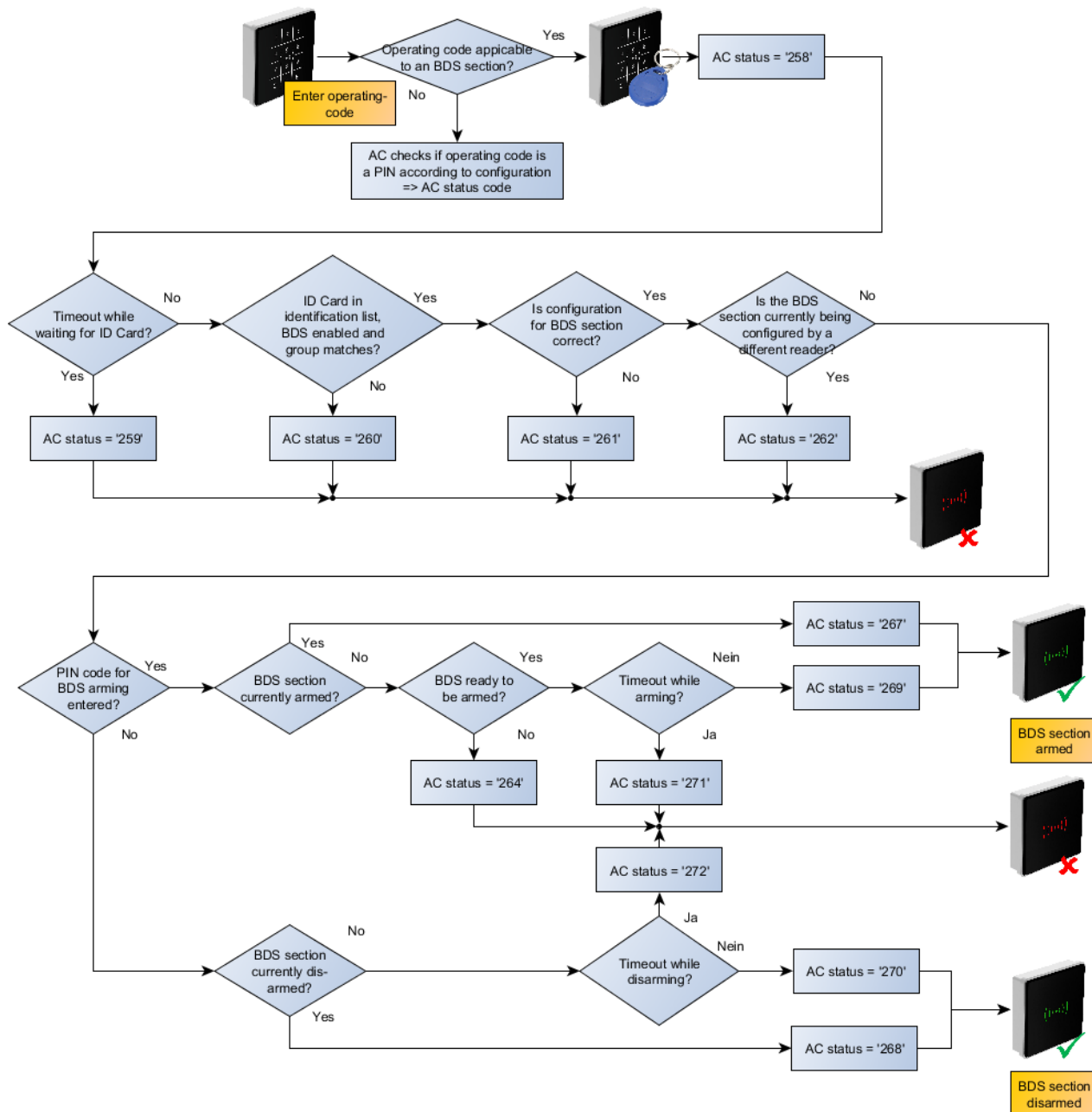
5.9.10.6. Statuscodes

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 ¹	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 nicht 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 ¹	Die EMA meldet per digitalem Eingang, dass sie zur Scharfschaltung bereit ist.
264 ¹	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 ¹	Der EMA-Bereich ist jetzt scharf.
270 ¹	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

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

5.9.10.7. 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. Berechnete 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

5.9.11. 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 ¹	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 nicht 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 ¹	Die EMA meldet per digitalem Eingang, dass sie zur Scharfschaltung bereit ist.
264 ¹	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 ¹	Der EMA-Bereich ist jetzt scharf.
270 ¹	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 -> Kommunikationskanal OK</td> </tr> <tr> <td>65</td> <td>Digi. Eingang3 Master High</td> <td>Digitaler Eingang3 Leser High</td> <td>Digi. 3; Sabotageüberwachung -> 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:

5.9.12. 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

5.9.13. Funktionen für ZK und U&Z

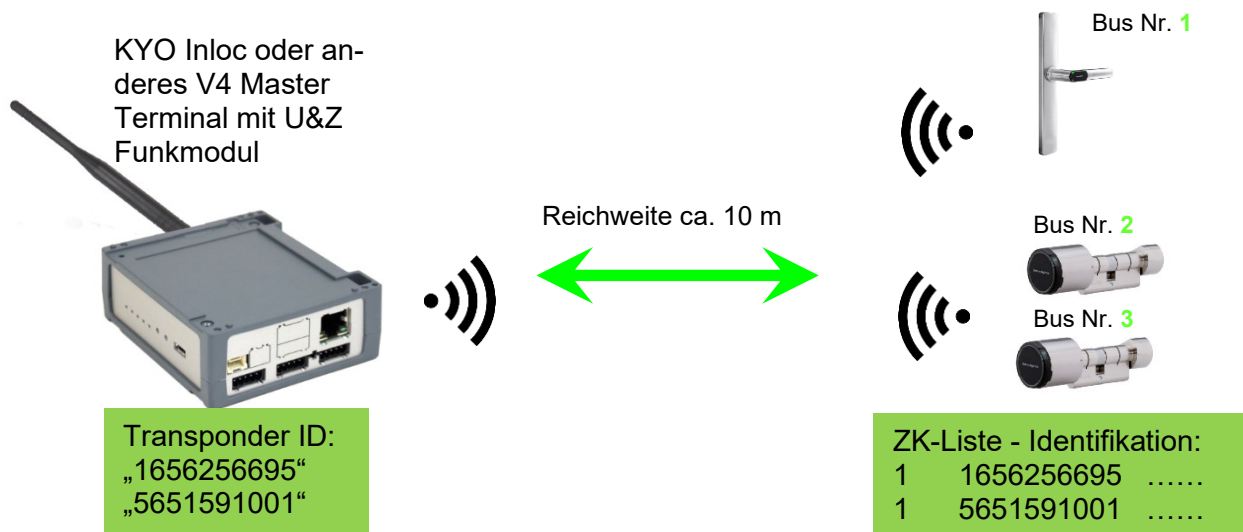
5.9.13.1. Aufbaubeispiel

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:



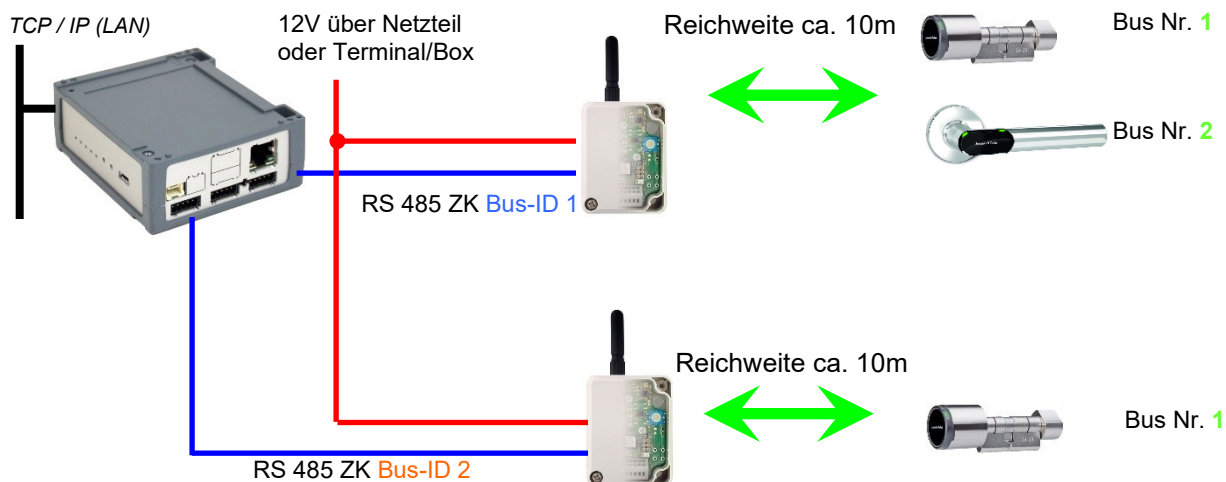
Die Transponder werden vom Zylinder gelesen und die ID an die ZK-Box übertragen. Diese entscheidet dann, ob die ID Zutritt erhält und sendet ein entsprechendes Signal an den Zylinder.

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 EVO 2.8 Pure V4 mit zwei externen Funkmodulen.

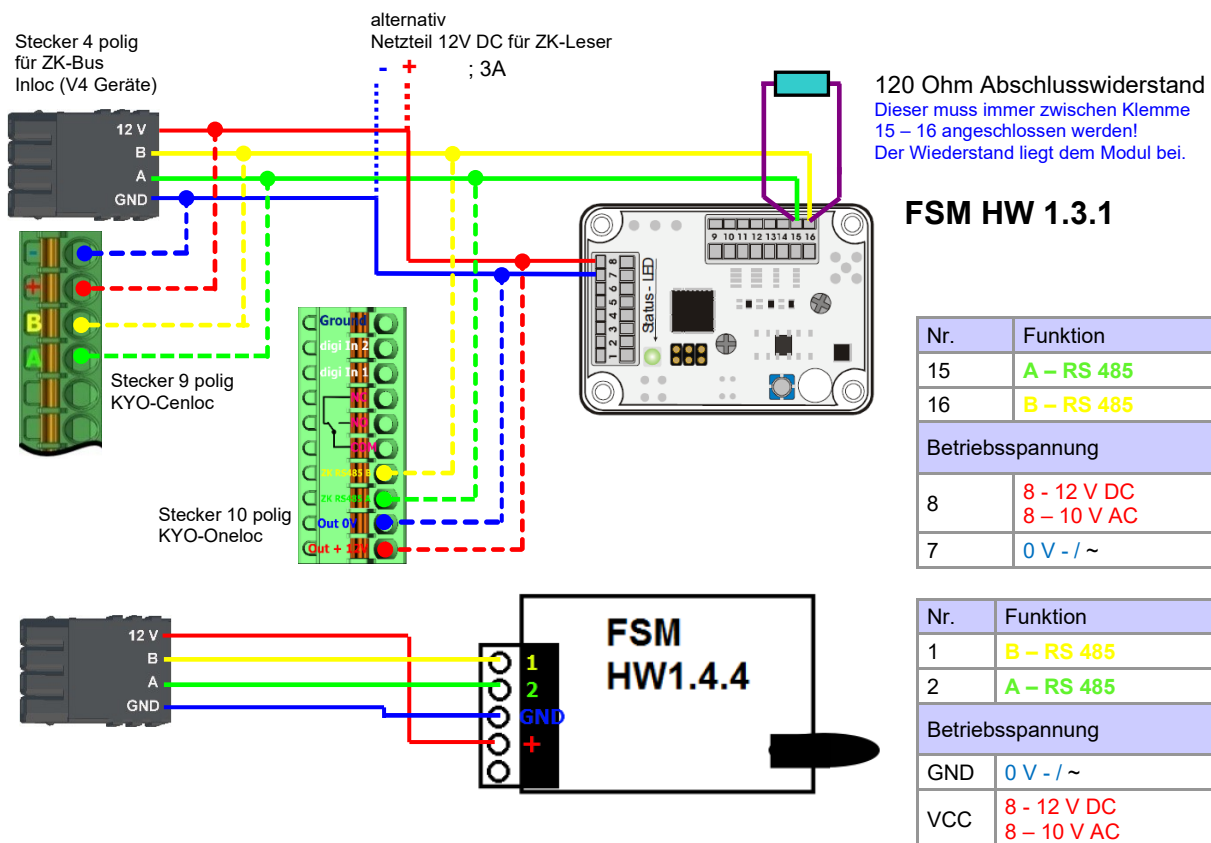


Entsprechende Reader Tabelle, Beispiel:

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)

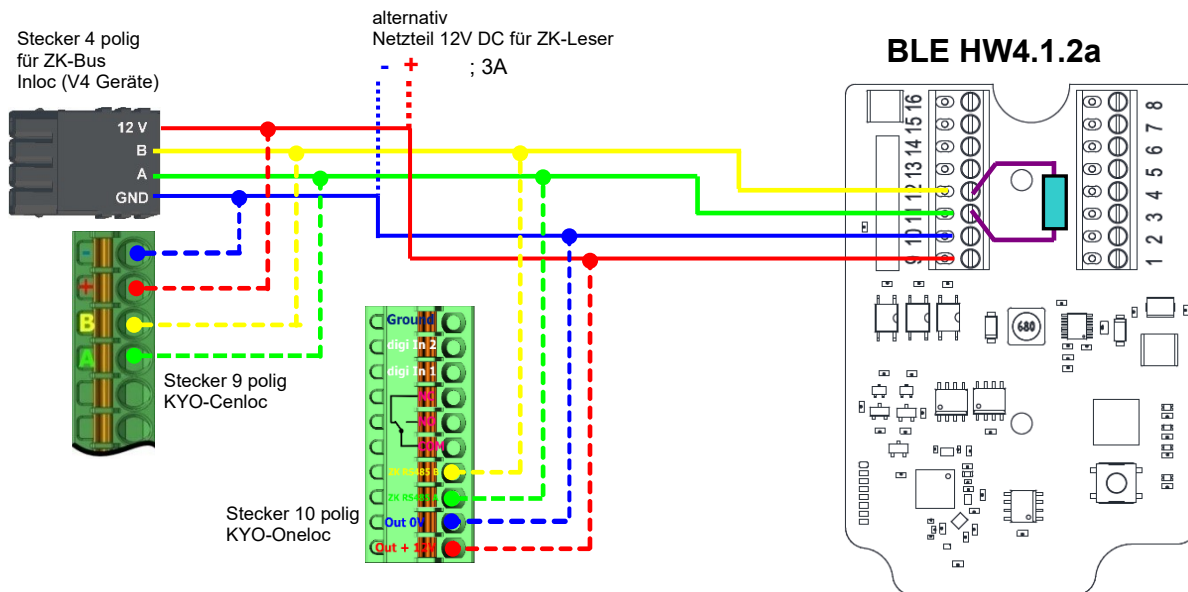
Verdrahtungsplan der verschiedenen ZK-Busanschlüsse mit externem Funkmodul 868 MHz:

(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

5.9.13.2. 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

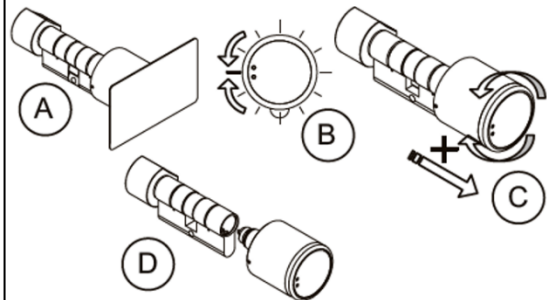
5.9.13.3. Montage und Demontage der Zylinder

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)

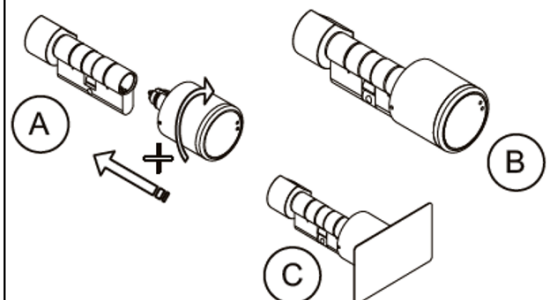
4.) Den Knauf durch geringfügiges Hin- und Herdrehen und gleichzeitiges leichtes Ziehen demontieren. (C+D)



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)

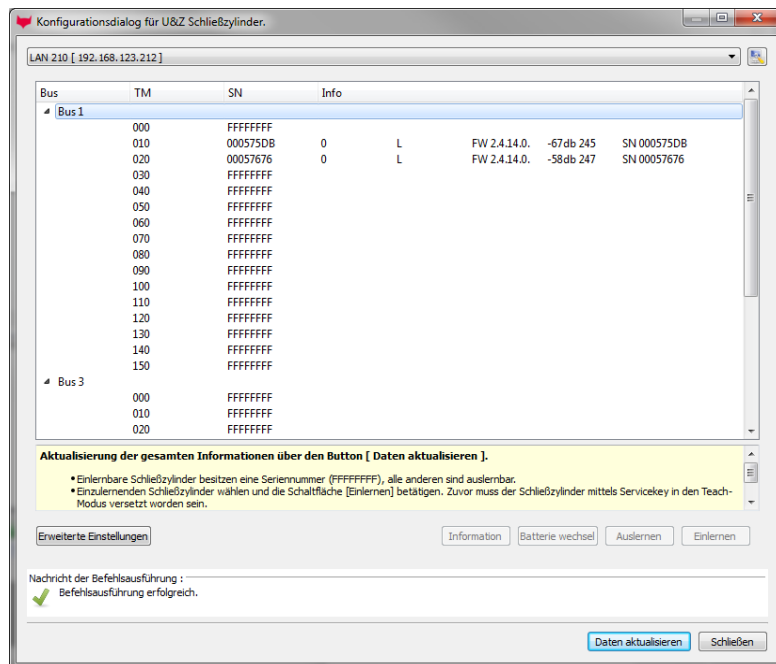
3.) Um den Demontagemodus zurückzusetzen, die Demontagekarte oder einen berechtigten Transponder vor das Knaufmodul halten. (C)



5.9.13.4. 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.

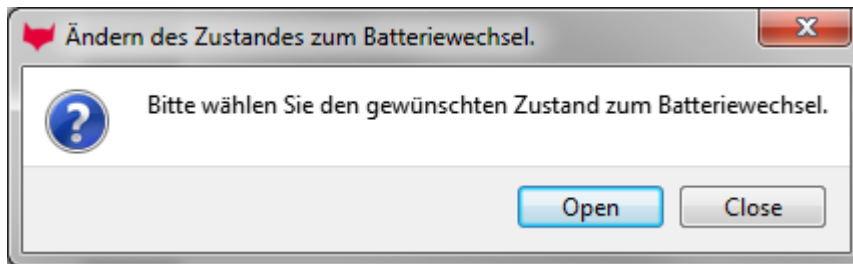
- Erweiterte Einstellungen
 - Festlegen der ZK-Master ID für das Gerät
 - KnobActiveTime: Zeit, die der Zylinder nach Aktivierung versucht das FSM zu erreichen, bis er wieder in den Standby geht
- Informationen zum einzelnen Schließzylinder (Spalte „Info“) aktualisieren
- Batteriewechsel versetzt den 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.

5.9.13.5. 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

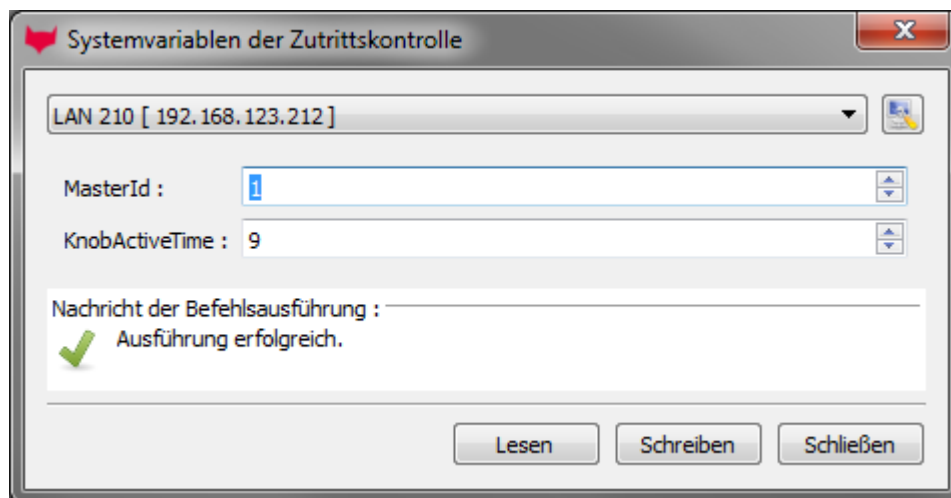
Das Knaufmodul reagiert nicht mehr auf berechnigte Ausweise. Ein Batteriewechsel ist unverzüglich vorzunehmen. Dieser ist nun nur noch mithilfe der Batteriewechselkarte möglich.

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

5.9.13.6. 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

5.9.13.7. 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

5.9.13.8. Optische und akustische Signale des U&Z Türdrückers

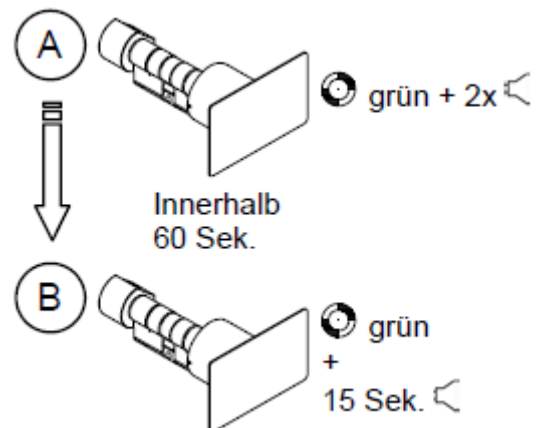
Funktion	Töne	Optische Signale
Ruhemodus		
Beginn Programmiermodus	- O	
Ende Programmiermodus	O -	
Ausweis angelernt	O O	●
Ausweis gelöscht	- -	●
Nach Wecken - Lesemodus		●
Ausweis nicht berechtigt	- - -	●
Ausweis berechtigt	O	●
Reset	-	● ●
Batteriewarnung Phase1	O O O O O	● ● ● ● ●
Batteriewarnung Phase2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

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

- = langer tiefer Ton
 O = kurzer hoher Ton

5.9.13.9. 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.



5.9.13.10.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 Unternehmens-standort 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!



Funk AUS !

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.

5.9.13.11. 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.

5.9.13.12. 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.

5.9.13.13. 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.

5.9.13.14. Technische Daten des Funkmoduls

Technische Daten CX 6932	
<p>Abmessungen Funkschaltmodul ohne Antenne: 65x50x40 mm Funkschaltmodul mit Antenne: 111x50x40 mm</p>	<p>Umweltbedingungen 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>Stromversorgung Versorgungsspannung: 8-20V= oder 8-16 V~ Stromverbrauch: Typ. 10mA (Ruhe), max. 50mA (Senden/Empf.)</p>	

5.9.14. 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).

5.9.15. 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“¹.

5.9.15.1. 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.

5.9.15.2. 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 grün². 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.

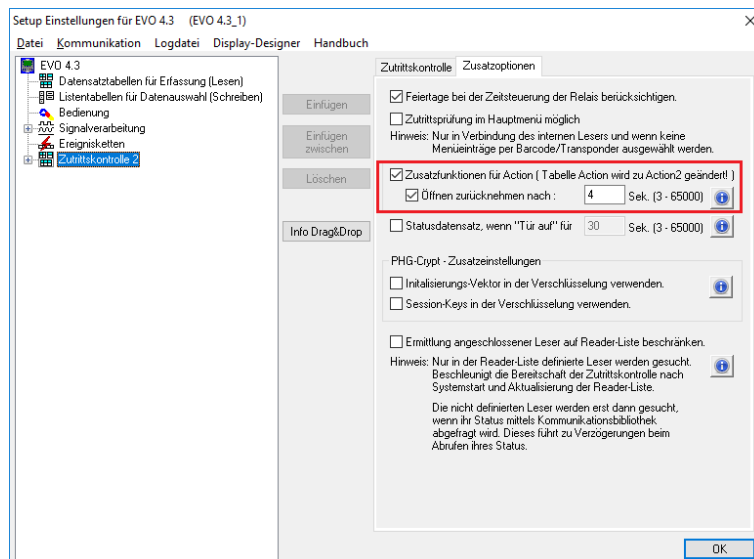
Hinweis: Bitte berücksichtigen Sie, dass das Aufbauen der Funkverbindung und damit das Prüfen, ob eine Tür aktuell im Betriebszustand „Dauer-Auf“ ist, eine bis zwei Sekunden in Anspruch nehmen kann. In dieser Zeit führt das Betätigen des Funk-Beschlags nicht zu einer Öffnung der Tür – die Tür kann erst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

¹ 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.

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

5.9.15.3. 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.

5.9.15.4. 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.

5.9.16. 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.

5.9.16.1. 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.

5.9.16.2. 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
123456	1	0	0	2022-01-01	2023-01-01	6

5.9.16.3. 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 nicht aktiv	Normale gültige Zutrittsbuchung oder erste Buchung eines Dauer-Auf-Ausweises	Klassischer Modus nicht aktiv	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 außerhalb des Buchungswiederholungszeitraums		Siehe 1	Siehe 1	
4		Zweite Buchung durch einen anderen Dauer-Auf-Ausweis innerhalb des Buchungswiederholungszeitraums				
5	Klassischer Modus aktiv	Zweite Buchung desselben Dauer-Auf-Ausweises innerhalb des Buchungswiederholungszeitraums	Klassischer Modus aktiv	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 außerhalb des Buchungswiederholungszeitraums				
8		Zweite Buchung durch einen anderen Dauer-Auf-Ausweis innerhalb des Buchungswiederholungszeitraums				
9		Zweite Buchung desselben Dauer-Auf-Ausweises innerhalb des Buchungswiederholungszeitraums	Klassischer Modus nicht aktiv	-	2x kurz blinken + 2x piepen	Wird dauerhaft ausgeschaltet

5.9.17. Bedienung /Aktivierung-Deaktivierung des Office-Mode

5.9.17.1. 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!

5.9.17.2. 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!

5.9.17.3. 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.

5.10. Transponderleser

Der Transponderleser ist im EVO 2.8 Pure integriert. Dass die Option vorhanden ist, erkennen Sie am Typenschild und durch das Etikett auf der Rückseite des Gerätes. Die Freigabe des Transponderlesens erfolgt durch die Einstellung im DatafoxStudioIV.

Siehe dazu mehr im Handbuch DatafoxStudioIV.

Um einem Transponder am Gerät zu lesen, halten Sie diesen vor das Gerät. Der Lesebereich ist mit diesem Zeichen gekennzeichnet.



Folgende Transponderleser können im EVO 2.8 Pure eingebaut werden:

EVO 2.8 Pure mit 125 kHz:	Unique EM4102, Hitag1, Hitag2, HitagS, Hewi EM4450 LRW 8 cm R/W (LeseReichWeite mit Karte)
EVO 2.8 Pure mit Legic-Prime/Advant:	LRW 4 cm R/W
EVO 2.8 Pure mit Mifare-Desfire:	LRW 4 cm R/W für MifarePlus / 7 Byte UID notwendig
EVO 2.8 Pure mit i-Button-Leser:	Touchmemory nur lesen
EVO 2.8 Pure mit HID 125kHz:	LRW 6 cm nur lesen ProxPoint Plus 4065
EVO 2.8 Pure mit HID-iCLASS:	LRW 4 cm nur lesen 13,56MHz
EVO 2.8 Pure mit Nedap:	LRW 4 cm nur lesen
EVO 2.8 Pure SimonsVoss Smart-Relais:	LRW optimal ca. 20 cm! Bei zu geringem Abstand, wird der Transponder ggf. nicht erkannt. (Schnittstelle Siemens: CLS-Signal=Ja).



Hinweis:

Ausführliche Anleitung zu den Einstellmöglichkeiten, finden Sie im Handbuch DatafoxStudioIV, in dem Kapitel „[Transponderverfahren](#)“.

5.11. Data on Card

5.11.1. Allgemeine Informationen

Mit der Funktion Data on Card ist es möglich, Daten mit einer individuellen Struktur auf einen Transponder zu schreiben.

Diese Daten werden in Form einer Liste von Ihrer Anwendung zur Verfügung gestellt.

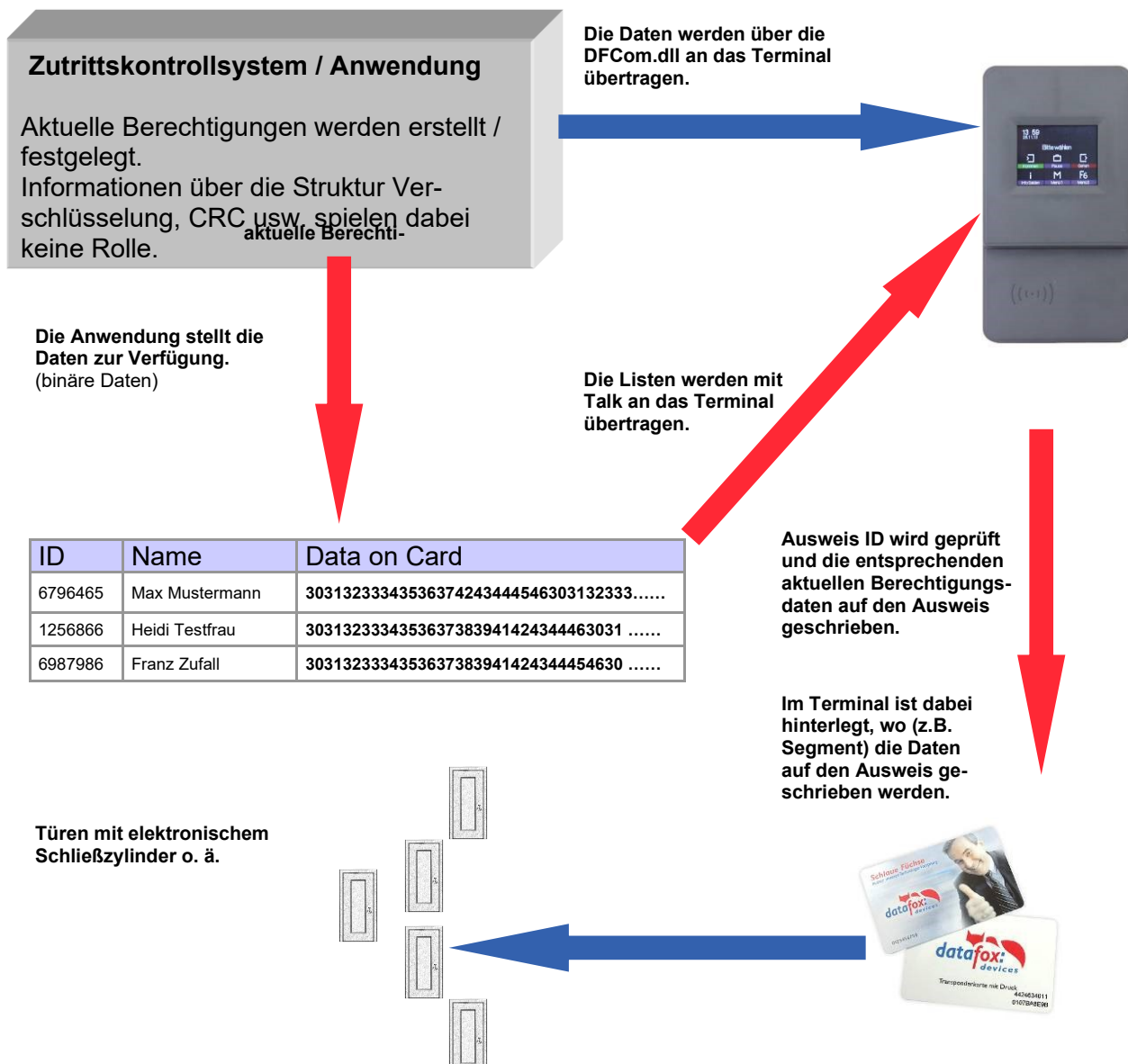
Diese Liste wird dann in das Terminal geladen und beim Vorhalten eines Transponders werden die Daten dann auf diesen geschrieben.

Folgende Transponderverfahren unterstützen die Funktion Data on Card:

- Mifare Desfire
- Mifare Classic (Einstellung Mifare Plus / auch Classic)
- Legic
- iCode
- MyD

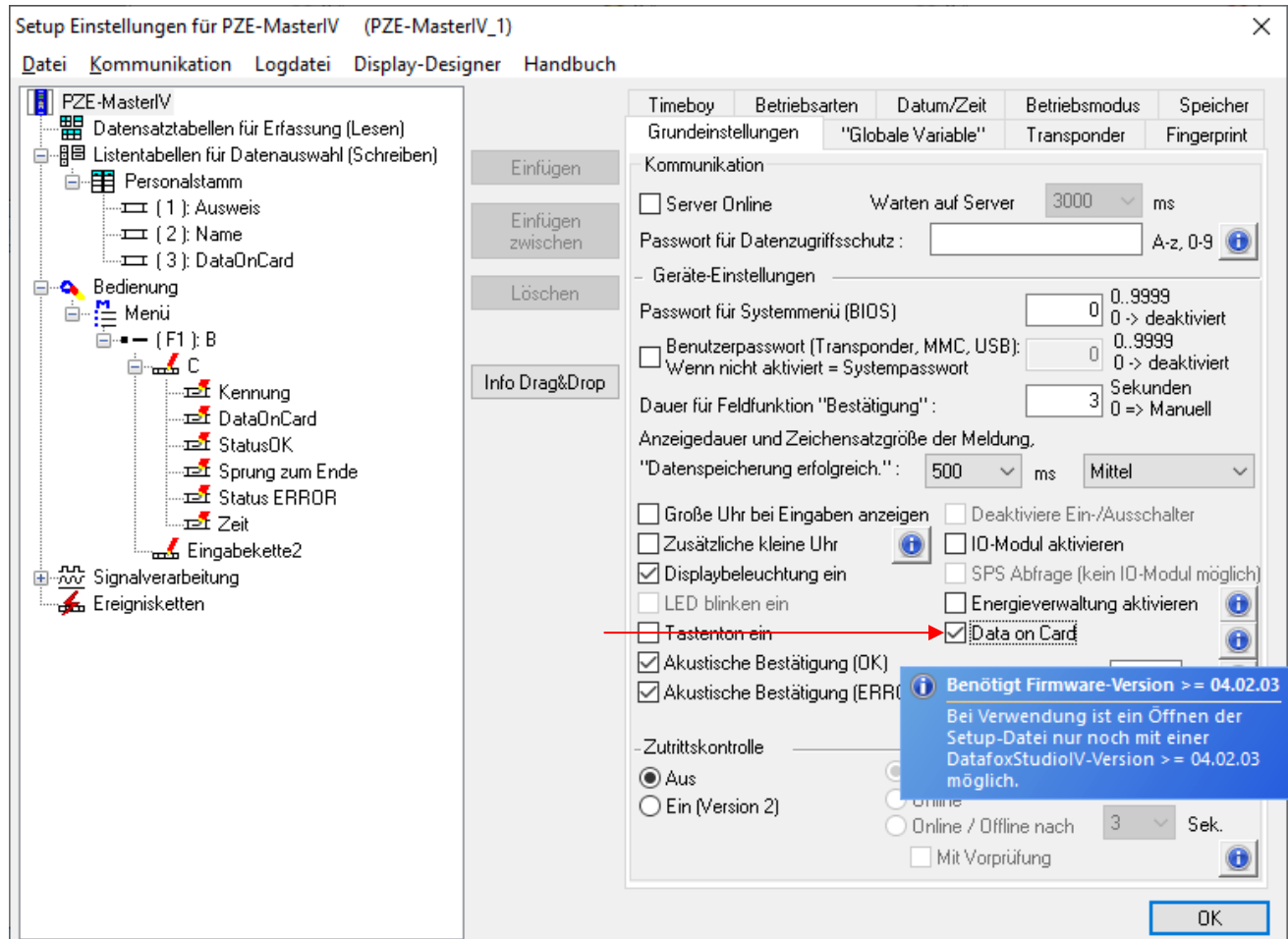
Folgendes Beispiel:

In Gebäuden mit „elektronischen“ Schließzylinder soll die aktuelle Tagesberechtigung für den Zutritt auf eine Transponderkarte geschrieben werden.



5.11.2. Einrichtung Data on Card

Data on Card ist eine Option des Gerätes bei der aus Listen Daten auf einen Transponder geschrieben werden können. Die Option muss bei der Bestellung mit angegeben werden. Bei Geräten die diese Option nicht haben, wird beim Ausführen eine Fehlermeldung angezeigt.



Data on Card arbeitet in **3 Schritten**:

- Lesen eines Wertes vom Transponder, z.B. Seriennummer.
- Der Wert wird zum Selektieren einer Liste mit Binärfeld benutzt um die binären Daten zu lesen.
- Die binären Daten werden auf den Transponder geschrieben.

Der Rückgabewert der Funktion Data on Card für GV oder Datensatzfeld ist der Wert aus dem ersten Schritt „Lesen eines Wertes vom Transponder“. Bei Fehlern wie „der Wert wird nicht in der Liste gefunden“ oder das „Schreiben auf den Ausweis schlug fehl“ erzeugt die Funktion ein ESC.

Über die Seite Sprünge kann dann entschieden werden, wie in der Eingabekette weiter gearbeitet wird.

Die binären Felddaten innerhalb der Datei, die das DatafoxStudioIV importiert und überträgt, sind als Hex Zeichenfolge anzugeben. Beim Importieren über die DLL sind die Daten als Binärdaten zu übergeben.

Über die Bearbeitungsfunktionen von Listendaten DFCGetField, DFCSetField arbeiten Sie mit Zeichenfolgen, wobei die Firmware eine Konvertierung der Hexstrings in und zu den Binärdaten vornimmt.

Einstellungen bei Data on Card

Setup Einstellungen für PZE-MasterIV (PZE-MasterIV_1)

1.) Transponderkonfiguration : Standard

2.) Liste mit den Daten : Personalstamm

3.) Transponderkonfiguration : Konfig 1

1.) Transponder Konfiguration Lesen

Setup Einstellungen für PZE-MasterIV (PZE-MasterIV_1)

Transpondertyp : Mifare DESFire

Global Standard Konfig 1

UID lesen (Seriennummer) auch von anderen Mifare Ausweisen.

Echte UID bei Random UID Ausweisen lesen.

UID mit 4 Byte Länge liefern

Applikation
 Nummer : 00000A Beispiel: App. 10 -> 00000A

Schlüssel
 1 Typ : TDES
 FFAACC11998864746767462376623472

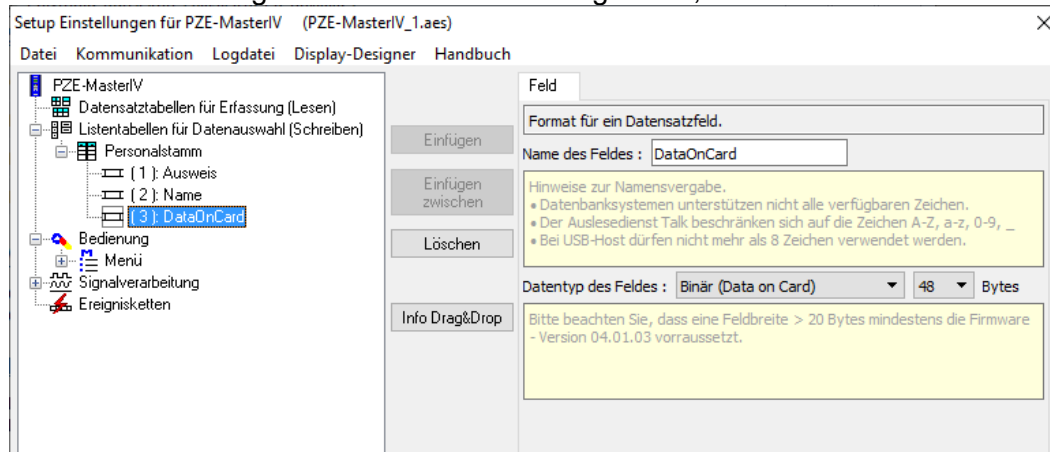
Datei
 Nummer Offset Anzahl Typ Komm. Mode
 1 0 0 Standard Plain

Ausgabeformat
 Hexadezimal Feste Länge : 0

Die Transponderkonfiguration für das Lesen kann frei gewählt werden. Sie muss aber zuvor in den Transpondergrundeinstellungen definiert worden sein.

2.) Listenkonfiguration

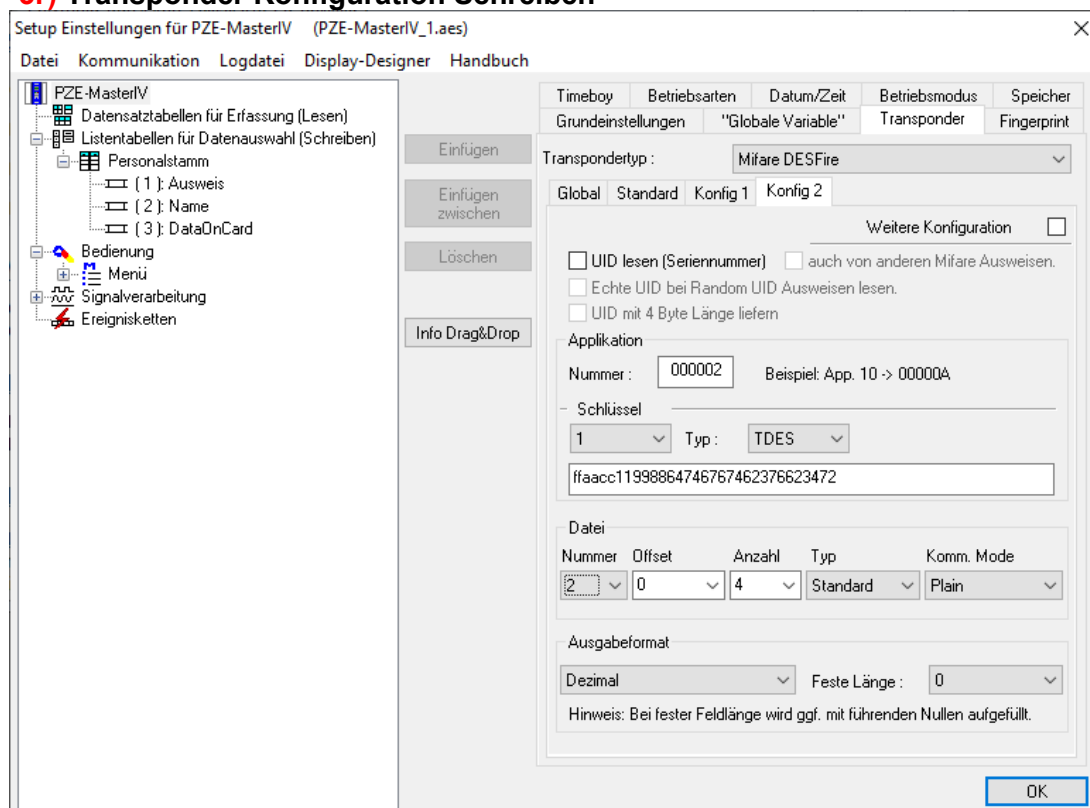
Bei der Listenkonfiguration wird die Liste ausgewählt, die ein Binärfeld hat.



In diesem Beispiel ist im Feld Ausweis der Wert vom Transponder Lesen, der in der Liste gesucht wird. Die zu schreibenden Daten sind im Feld Data on Card vom Typ Binär. Die max. Feldgröße darf 220 Byte nicht überschreiten.

Anschließend kann noch bei Listenfehlern die weitere Verfahrensweise festgelegt werden.

3.) Transponder Konfiguration Schreiben



Die Transponderkonfiguration für das Schreiben kann frei gewählt werden, sie muss aber zuvor in den Transpondergrundeinstellungen definiert worden sein.



Hinweis:

Zuerst die Transponderkonfiguration fertig stellen, dann die Liste mit dem Binärfeld anlegen und zum Schluss die Feldfunktion Data on Card parametrieren.

Beispiel für Data on Card:

Ausweis mit Seriennummer **1848989745**

Listeneintrag für **1848989745** in der Datei vor dem Übertragen in das Gerät

Feld ID Feld Data(Binärfeld) hier als Hex-Bytes

1848989745 30313233343536373839414243444546303132333435363738394142434445463031323334353637383941

Daten nach Konvertierung bzw. innerhalb des Gerätes

Feld ID Feld Data(Binärfeld) hier binär

1848989745 0123456789ABCDEF0123456789ABCDEF0123456789A

Auf den Ausweis werden folgende Daten geschrieben

0123456789ABCDEF0123456789ABCDEF0123456789A

Binär sehen die Daten so aus:

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

Hinweis:

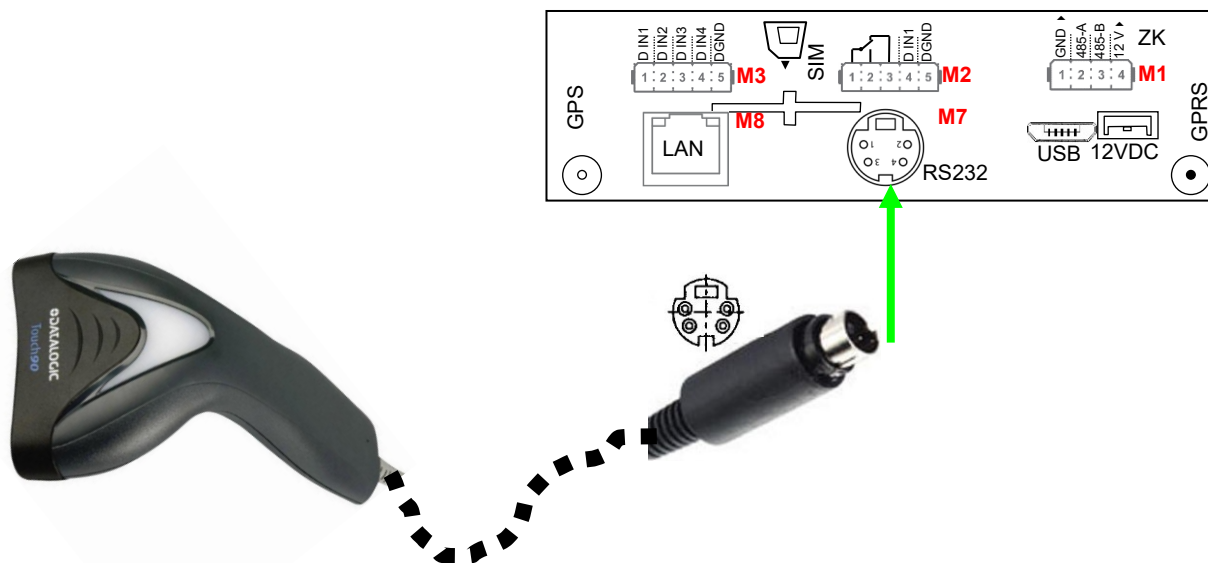


Bei einer Signalisierung von 3 langen Tonfolgen, steht die Option Data-On-Card an diesem Gerät nicht zur Verfügung.

Hier muss die Option nachträglich erworben werden.

5.12. Barcode Leser für V4 Terminals

Sie können alle Barcodeleser mit einem RS232-Anschluss an das EVO 2.8 Pure anschließen. Beachten Sie dabei die nachfolgend aufgeführte Anschlussbelegung der RS232-Schnittstelle.



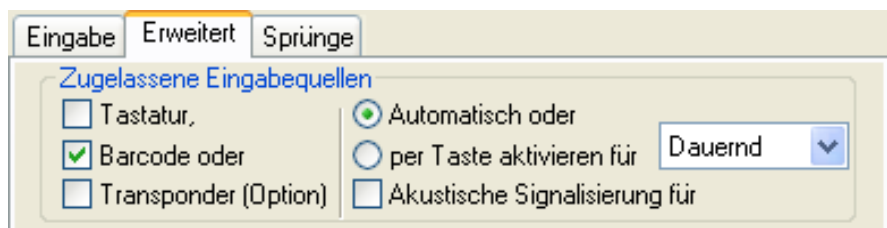
Beschreibung	Modulplatz	PIN	Funktion
RS 232 Mini-DIN M004	je nach Aus- stattung hier M7	1	TXD
		2	RXD
		3	+ 5 V
		4	Ground / GND

Barcodes die eingelesen werden, können bis zu 255 Zeichen lang sein. Dies wird durch die Feldfunktion „Normal (Wertübernahme von Transponder usw...)“ unterstützt.

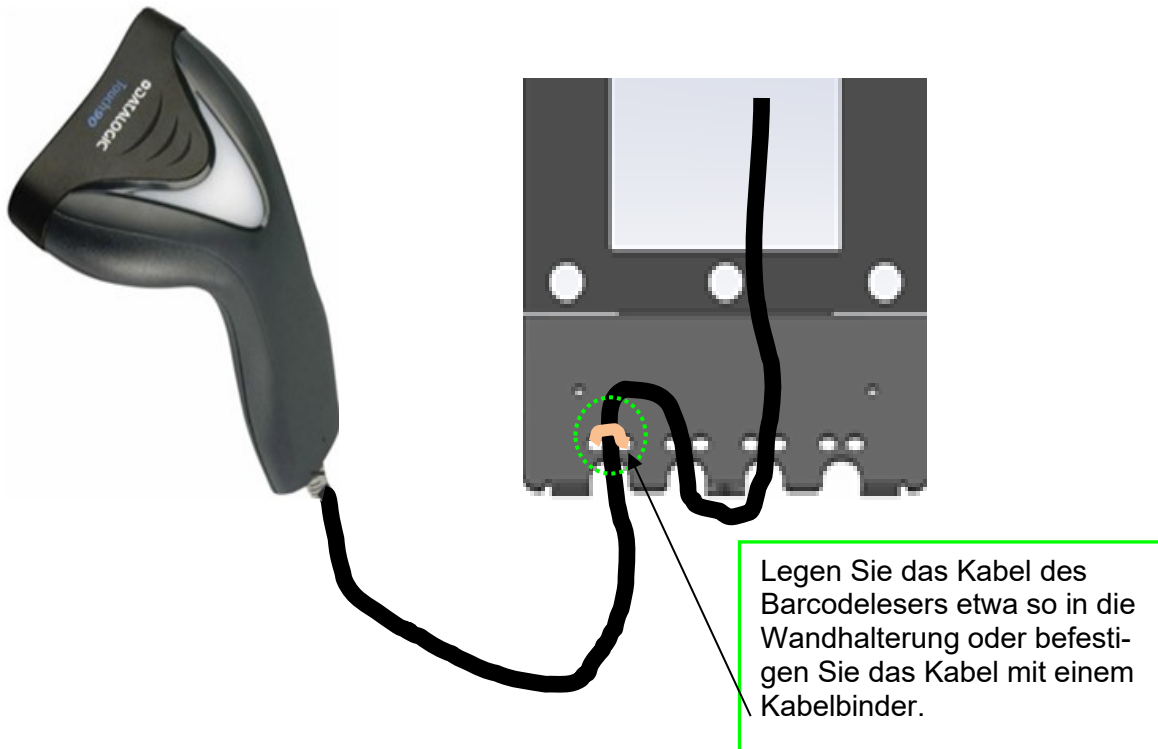
Alle (bis max. 255) Zeichen werden im Zwischenspeicher des Gerätes gehalten. Daraus können nun je nach Bedarf bis 60 Zeichen zusammenhängend ausgeschnitten werden und z.B. in einer GV gespeichert werden.

Mehr Informationen über das die Zuschneidefunktion finden Sie im Handbuch DatafoxStudioIV unter dem Kapitel „Feldfunktionen im Gerätesetup“ → „Normal (Wertübernahme von Transponder usw...)“.

Einstellung im DatafoxStudioIV:



Zugentlastung für das Kabel des Barcodelesers:



5.13. Fingerscanner, EVO

Auf vielfachen Kundenwunsch haben wir einen neuen Fingersensor (Optisch) in unser Programm aufgenommen. Dabei handelt es sich um einen optischen Flächensensor.

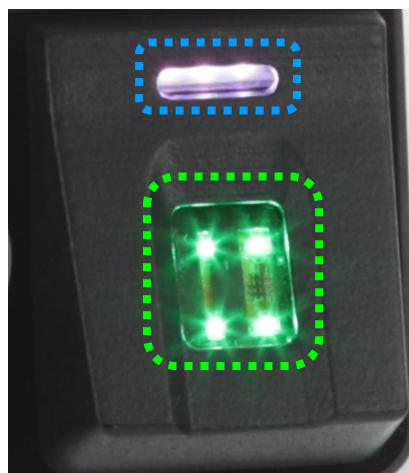
RGB LED

Die Steuerung der LED erfolgt durch das Setup des Gerätes.
Siehe Feldfunktion
„Hintergrundbeleuchtung schalten“.

Optischer Flächensensor.

Hinweis:

Die Hintergrund LED-Beleuchtung ist nur an, wenn ein Finger auf den Sensor aufgelegt wird.



Mit dem Sensor wurde auch eine neue Menüführung für das Einlernen und Löschen der Finger eingeführt. Das Menü wird automatisch aufgerufen, wenn die Feldfunktion Administration im Setup (Gerätekonfiguration) aufgerufen wird.

Das Menü enthält 6 Seiten: **Finger prüfen, Finger einlernen, Finger trainieren; Einzelne Finger löschen und Alle Finger löschen. Zusätzlich kann Finger auf Karte schreiben aktiv sein.**

Eingabe
Sprünge

Eine Funktion für Feld- und/oder GV-Zuweisung ausführen

Name der Feldabfrage:

Text in Zeile 4 der Anzeige:

Name des Feldes

v

Feldbezeichnung, entsprechend

nicht gewählt

v

Feldfunktion :

Fingerprint: Finger Administration

v

"Globale Variable" mit PID :

GV: Ausweis

v

Ein- und Ausblenden von Seiten

- Finger prüfen
- Finger einlernen
- Finger trainieren
- Einzelne Finger löschen
- Alle Finger einer Person löschen
- Finger auf Karte schreiben

Die einzelnen Menüpunkte können Sie wählen!

Die Handhabung des neuen Fingersensors können Sie auch in unserem Video betrachten.

<https://www.datafox.de/video-verwendung-und-einlernen-einer-fingerprintloesung-mit-optischen-flaechensensor.de.html>

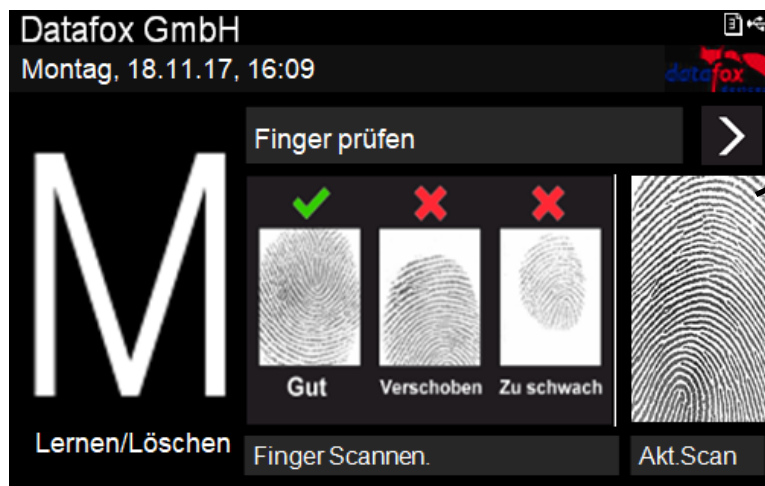
! Alle Terminals sollten so montiert werden, dass sich der Fingersensor in der gleichen Höhe befindet, damit die Handhabung identisch erfolgen kann.

! Der Fingerscanner kann nur mit der Einstellung EVO-Liner Displaylayout genutzt werden. Im **PZE-Layout** wird der Fingerscanner **nicht** unterstützt.

5.13.1. Menüseite Finger prüfen

Diese Seite dient dazu herauszufinden, welcher Finger das beste Scanergebnis liefert und wie der Finger am besten aufgelegt werden sollte. Hierzu legen Sie den Finger möglichst gerade mit leichtem Druck auf den Sensor. Der wichtigste Bereich ist die Mitte des vordersten Fingerglieds. Suchen Sie in Ruhe die Finger aus, die das bestmögliche Bild liefern. Bitte beachten Sie die Bilder und [Hinweise](#) im Anschluss.

Wenn das Bild insgesamt zu blass ist, könnte das an der Trockenheit des Fingers liegen. Leichtes Reiben oder Anhauchen der Fingerspitze verbessert das deutlich, siehe auch die Beispielbilder unten.



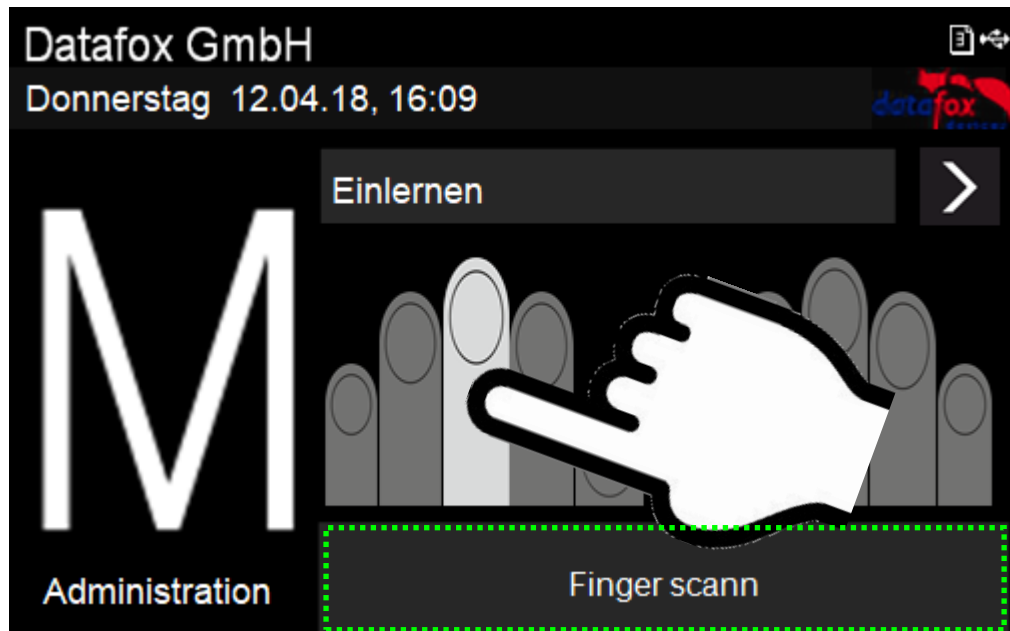
Ist der Finger gescannt, wird das entsprechende Bild hier dargestellt.

Bitte vergleichen Sie mit den [Bildern nebenan](#), ob das Bild ausreichende Qualität bietet.

Haben Sie die entsprechenden, geeigneten Finger ausgesucht, drücken Sie auf den Pfeil , um auf die nächste Seite zu wechseln.

5.13.2. Menüseite Finger „Einlernen“

Wählen Sie den Finger den Sie einlernen möchten, indem Sie einfach auf den entsprechenden dargestellten Finger im Display tippen! Die dunkelgrauen Felder sollen die beiden Hände symbolisieren, die Daumen sind in der Mitte.



Bei den Geräten EVO 2.8/3.5 ist dieser Bereich gleich die „ENTER“-Taste.

Folgen Sie den Anweisungen im Display.

Der Finger muss 3-mal gescannt werden. Nach jedem Piepsen müssen Sie den Finger kurz vom Scanner anheben und wieder auflegen.

Das erfolgreiche Einlernen wird durch ein grünes Feld angezeigt, in dem auch ein Qualitätswert steht. Bei einem Qualitätswert von 85 und mehr war das Einlernen sehr erfolgreich.

Bei niedrigeren Werten kann das Einlernen direkt wiederholt werden, um eventuell ein besseres Ergebnis zu erreichen. Das Einlernen sollte mit einem möglichst hohen Qualitätswert abgeschlossen werden, da es die Grundlage für die spätere Erkennung ist.

Natürlich gibt es Finger, die nur niedrigere Werte erreichen können. In diesem Fall sollten aber auch andere Finger dieser Person getestet werden.

Wir empfehlen, für jeden Benutzer mindestens zwei Finger einzulernen, falls ein Finger aufgrund einer Verletzung nicht erkennbar sein sollte.

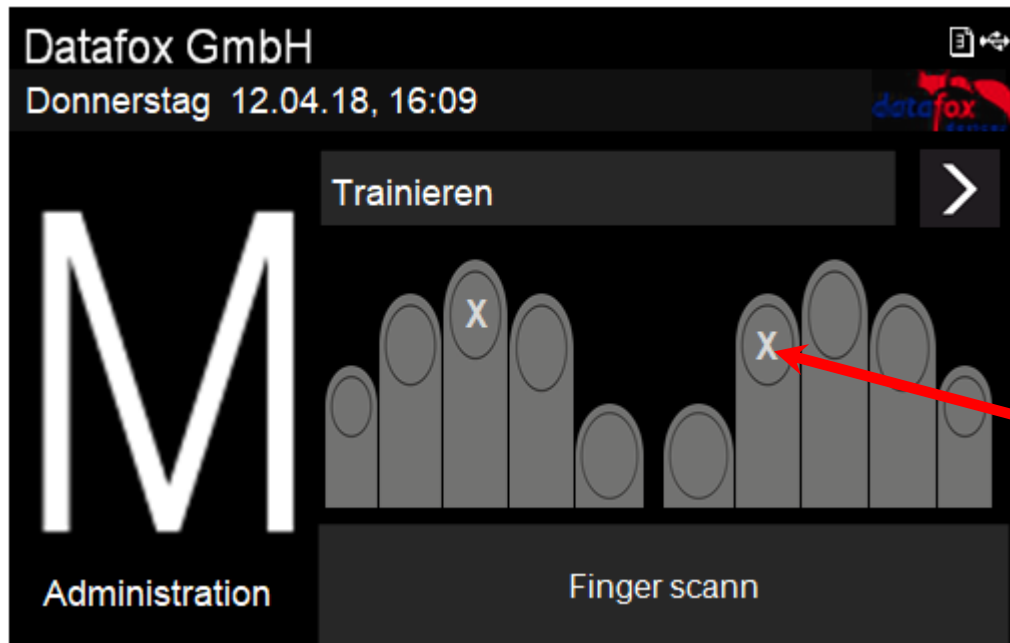
Durch die Auswahl eines anderen Fingersymbols können im Anschluss direkt weitere Finger einge-
lernt werden.

5.13.3. Menüseite „Trainieren“

Dieser Schritt erfüllt zwei Aufgaben, zum einen eine Funktionskontrolle, dass die eingelernten Finger auch tatsächlich erkannt werden, zum anderen kann das System noch weiter optimiert, also trainiert werden.

Zum Optimieren sollen die Finger nun bewusst etwas verschoben oder verdreht aufgelegt werden. Dadurch wird nach und nach ein größerer Bereich des Fingers erkannt und somit das abgespeicherte Template optimiert. Eine Optimierung wird durch den grünen Balken angezeigt. Gut für das System ist, wenn mehrere solche Optimierungen zu einem Finger erfolgen können.

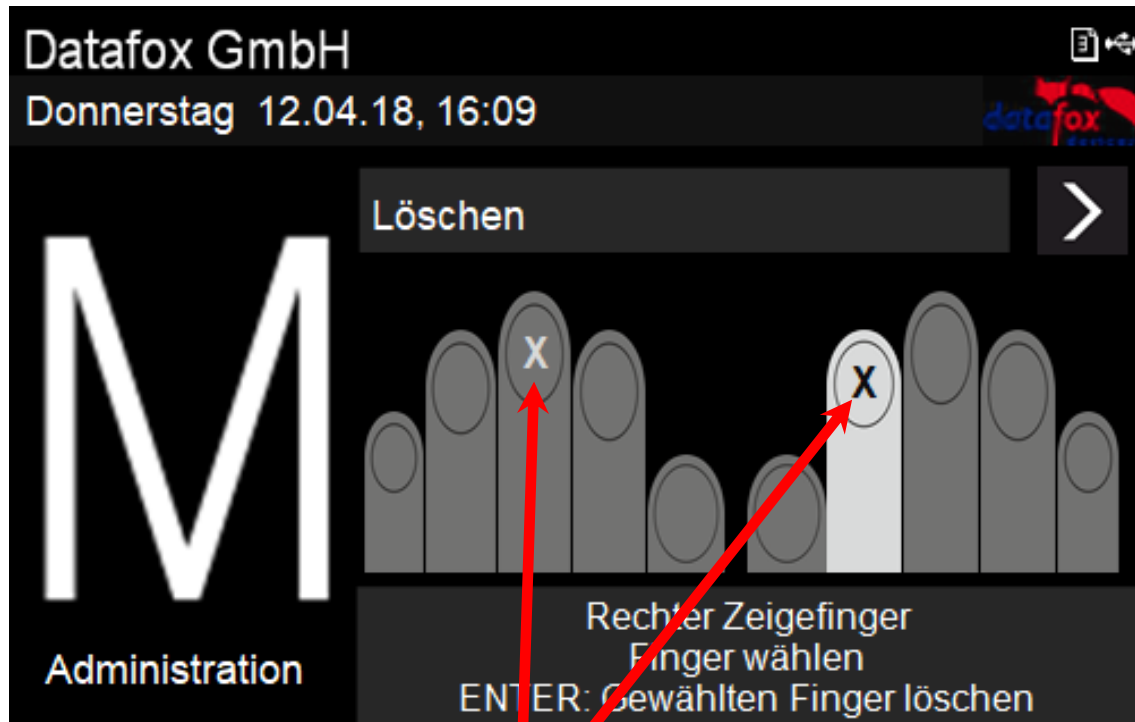
Wenn keine grünen Rückmeldungen mehr kommen, kann das Trainieren beendet werden.



Die bereits eingelernten Finger sind mit „X“ gekennzeichnet.

5.13.4. Menüseite „Löschen“

Löschen von einzelnen Fingern:



Die eingelernten Finger sind mit „X“ gekennzeichnet.
Tippen Sie auf den Finger den Sie **löschen** möchten und bestätigen dies mit „**Enter**“

Alle Finger einer Person löschen:

Auf der nächsten Menüseite „Alle Finger einer Person löschen“ werden alle eingelernten Finger der Person hervorgehoben dargestellt. Beim Bestätigen durch Enter werden sämtliche Finger der Person vom Fingerprint-Sensor entfernt.

5.13.5. Menüseite „Beenden“

Für EVO 2.8 und 3.5 gibt es eine separate Seite zum Beenden des Finger-Administrations-Menüs. Klicken Sie einfach auf die Mitte des Displays und das Menü zu verlassen.

Bei EVO 4.3 können Sie durch Drücken der „ESC“-Taste das Administrations-Menü verlassen.

5.13.6. Hinweise zur Verwendung des Fingerprint-Flächensensors

5.13.6.1. Hints for using the fingerprint area sensor

Dieser Abschnitt zeigt anhand von Fingerprint Bildern, wie sie auch beim „Finger check“ angezeigt werden, wie ein Bild aussehen sollte und welche Auswirkungen durch schlechte Position, falschen Druck oder ungünstige Finger erkennbar sind.

This chapter shows with images, as they are also shown in the function “Finger check” how a good image should look like and how they could look with respect to bad positions, bad pressure or difficult fingers.

- Der Finger muss mit leichtem Druck auf den Sensor gelegt werden.
The finger must be put onto the sensor with light pressure.
- Der wichtigste Bereich ist die Mitte des vordersten Fingerglieds, da dort die meisten Eigenschaften vorhanden sind.
The most important area is the middle of the front phalanx, because there are the most characteristics.
-

Gutes Bild / good image



Schlechte Positionen / Bad positions

Zu weit unten
Too far down



Zu weit oben
Too far up



Zu weit links
Too far left



Zu weit rechts
Too far right



Schlechter Andruck / **Bad pressure on the sensor**

Zu wenig Druck
Too little pressure



Zu viel Druck
Too much pressure



Finger verdreht / **Finger twisted**

Zu steil, nur Finger-
spitze
**Too steep, only finger-
tip**



Nach links verdreht
Twisted to left



Nach rechts verdreht
Twisted to right



Schräg rechts /
Diagonally right



Trockene Finger / **dry fingers**

Finger sehr trocken
Finger very dry



Trockenen Finger kurz
gerieben
**Dry finger shortly
rubbed**



Trockenen Finger an-
gehaucht
Dry finger breathed on



Trockenen Finger ein-
gecremt
Dry finger with cream



Schwierige Finger / Difficult fingers

Falten /
Wrinkels



Unterbrechungen /
Interruptions



Falten, unscharf
Wrinkels, diffuse



Unscharf /
Diffuse



Schwierige Finger / Difficult fingers

Generell Undeutlich /
Generally unclear



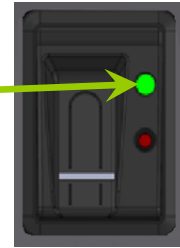
Fingerprint Flächensensor Saturn01

Templates	5000 Templates à 640 Byte, ISO19794-4; ANSI-378	Im Modul können 5000 Finger verwaltet werden, ein Template hat 640 Byte.
Auflösung	500 dpi	Die Sensor-Auflösung beträgt 500 dpi
Aktive Fläche	14 x 18mm	Die aktive Fläche des Sensors beträgt 14 x 18mm.

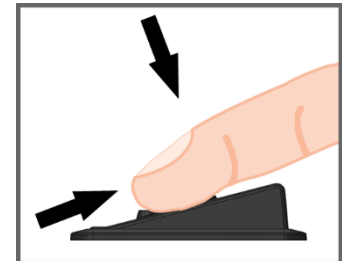
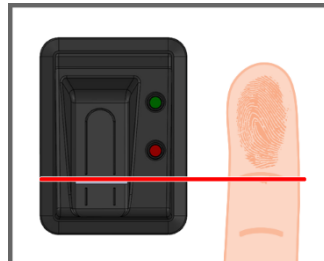
5.14. Fingerscanner mit Zeilensensor

5.14.1. Bedienung Fingerscanner

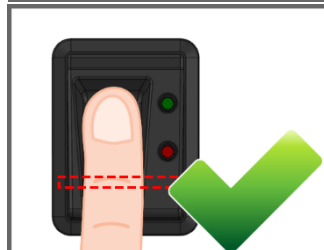
Die Scanbereitschaft des Fingerprintlesers wird durch die blinkende grüne LED signalisiert.



1.) Den Finger im Bereich des vorderen Gelenks auflegen.



2.) Den Finger flach auflegen. Achtung nicht verkantet auflegen, weil sonst nur ein Teil erfasst werden kann.



3.) Den Finger mit etwas Druck auf den Scanner flach über den Scanner ziehen.

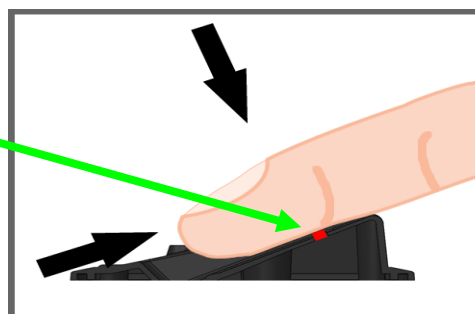


Um eine gute Erkennung des Fingers zu ermöglichen, müssen die Finger sauber sein!

Achtung!

Dieser kleine Streifen, hier rot dargestellt, ist der eigentliche Zeilenscanner.

Den Finger mit leichtem Druck über den Sensor ziehen. Der Kontakt vom Finger zum Scanner darf dabei nicht



Schnitt-Ansicht

So Scannen Sie richtig Videoanleitung: <http://www.datafox.de/videothek.html>



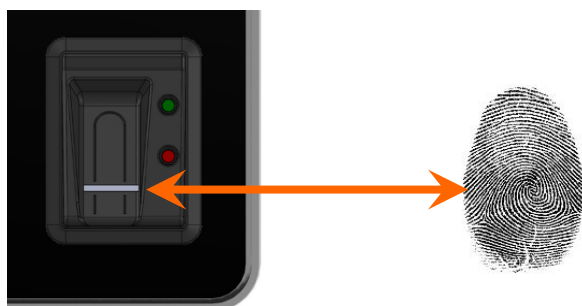
Alle Terminals sollten so montiert werden, dass sich der Fingersensor in der gleichen Höhe befindet, damit die Handhabung identisch erfolgen kann.



Auf gar keinen Fall dürfen Bestandteile am Finger sein, die eine schmirgelnde Wirkung haben. Diese nutzen die Schutzschicht des Zeilensensors ab und vermindern damit die Lebensdauer erheblich.

5.14.2. Allgemeine Informationen

Biometrie bietet die Möglichkeit mit körpereigenen Merkmalen eine Identifizierung oder Verifizierung vorzunehmen. Datafox unterstützt mit dem Fingerprint-Modul die Fingererkennung. Man benötigt so keinen Ausweis mehr, und kann diesen dann auch nicht vergessen und einen PIN muss man sich auch nicht mehr merken. Die Buchung per Fingerprint ersetzt also das Lesen des Ausweises. Die Terminals unterstützen hier selbstverständlich auch alle anderen Funktionen, wie bei der Buchung mit dem Ausweis. Dieses Datenblatt stellt damit eine Ergänzung des jeweiligen Produkt-Prospekts dar.



Grundsätzlich ist zwischen folgenden Informationen zu unterscheiden:

Die „PID“ ist die Personen Identifikations Nummer, auch als Mitarbeiter-Nr. bekannt. Zu einer PID können max. 10 Fingertemplates zugeordnet werden. Die PID sollte immer eine dezimale Zahl sein, also muss beim Einsatz von Transpondern das entsprechende Format (Dezimal n Stellen) ausgewählt werden.



Achtung:

Die PID darf den dezimalen Wert von 4294967295 ($2^{32} - 1$) nicht überschreiten. Wir empfehlen daher mit einer 9-stelligen PID zu arbeiten.

Das „Fingertemplate“ setzt sich aus der PID und den Fingereigenschaften einer Person zusammen. Die Fingereigenschaften sind die Merkmalspunkte (Minutien), die aus dem Bild nach dem Scannen eines Fingers ermittelt werden konnten.

Die „Sicherheitsstufe“ (Fehlerakzeptanzrate/Fehlerrückweisungsrate) legt fest, wann ein gelesener Finger akzeptiert bzw. abgelehnt wird. 60 bedeutet, dass 60% der Minutien des gescannten Templates mit 60% des Referenztemplates übereinstimmen müssen, damit eine Erkennung als gültig erklärt wird. Empfehlung nicht unter 55 und über 75 einstellen. Am besten 60 benutzen.

Bildqualität ist die Anzahl der nutzbaren Fingerlinien zur Anzahl der zur Verfügung stehenden Fingerlinien. Empfehlung nicht größer als 40 wählen.



Achtung:

Bei der Bildqualität ist der empfohlene Wert 40. Bei älteren Modellen mit Biokey 3000 mit einem Firmwarestand 04.12 ist der empfohlene Wert 70. Biokey 3000 mit Firmware 61.00 muss die Bildqualität unbedingt kleiner 70 sein. Der von uns empfohlene Wert von 40 bietet ein Optimum zum Einlernen der Finger.

Die „Anzahl Minutien“ gibt an, wie viele Minutien aus dem Bild ermittelt werden müssen, damit ein Template für einen Vergleich (Matching) erstellt werden bzw. als gültig erklärt werden kann. Empfehlung nicht kleiner als 7, besser 10 einstellen.

**Hinweis:**

Empfohlene Einstellungen:

Sicherheitsstufe: 60%, Bildqualität: 40% Mindestanzahl Minuten: 15

Bei schwierigen Fingern kann durch verringern der Parameter eine Erkennung erreicht werden, das kann aber zu Falscherkennungen führen. Das Verhalten muss in jedem Einzelfall geprüft werden, da es sehr stark vom Personenkreis abhängig ist.

Bei solchen Fällen, sollte man auf einen anderen Finger ausweichen, weil nicht jeder menschliche Finger für das Minuten -Verfahren geeignet ist.

5.14.3. Einlernen

Um Fingerprint nutzen zu können, müssen zunächst die Personen am Terminal eingelernt werden.

Die 4 Schritte des Einlernens

Schritt 1
Ermitteln der PID

Transponder oder Listenauswahl → PID



Listentabellen für Datenauswahl
 Personal
 (1): PersonalNr
 (2): PersonalName

Ausweis-Nr	Name
00799611485215	M. Mustermann
05597861113494	M. Musterfrau

Schritt 2
Finger scannen

Fingerprint: Scannen.



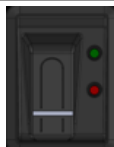
Schritt 3
PID mit Fingereigenschaften verknüpfen

Feldfunktion:

PID + Fingereigenschaften = Template

Schritt 4
Template speichern

im Biokey-Modul



auf Mifare Transponder



auf Server



5.14.4. Verfahren

Identifikation

Die Fingereigenschaften werden über das Fingerprint Modul erfasst. Anschließend wird der Datenbestand auf Übereinstimmung geprüft. Bei festgestellter Übereinstimmung wird die PID der identifizierten Person zurückgeliefert, andernfalls ein Fehler. Die Schwelle der Übereinstimmung legt die Sicherheitsstufe fest.

Verifikation

Ein Mitarbeiter identifiziert sich durch einen Transponder. Hierbei wird die PID (Mitarbeiter-Nr) vom Ausweis gelesen. Anschließend muss der Mitarbeiter seinen Finger über den Scanner des Fingerprint Moduls ziehen. Im Datenbestand des Fingerprint Moduls werden nun alle Primärschlüssel (Kombination aus PID und Template) mit dieser PID ermittelt und auf Übereinstimmung mit den gescannten Fingereigenschaften geprüft. Hierbei sind bis zu zehn Zuordnungen möglich.

Vorteil: Die Erkennung geht schneller und die Sicherheit steigt.

Nachteil: Ein weiteres Erkennungsmedium (z.B. Transponder) wird benötigt.

Identifikation mit Datenhaltung der Fingertemplates im Fingerprint

Das Terminal pollt den Fingerprint regelmäßig an, ob jemand einen Finger eingelese hat. Wenn ja, übergibt der Fingerprint dem Terminal, wer das war und ob der Finger gültig war. Dabei werden die PID und die Gültigkeit übergeben. Der Task im Terminal für den Fingerprint löst, falls im Setup definiert, eine Eingabekette oder eine Zutrittsprüfung aus. Wird keine Person erkannt, liefert der Fingerprint eine PID = 0.

Verifikation mit Datenhaltung der Fingertemplates im Fingerprint

Das Terminal pollt regelmäßig den Transponderleser an, ob ein Transponder vorgehalten wurde. Wenn ja, wird die Seriennummer oder ein Speicherbereich des Transponders an den Fingerprint übergeben. Dieser wartet dann auf das Einlesen eines Fingers. Nach dem Einlesen des Fingers wird geprüft, ob der mit der Seriennummer bzw. übergebenen Transponderdaten hinterlegte Finger im Fingerprint mit dem eingelesenem übereinstimmt. Der Fingerprint übergibt an das Terminal PID und die Gültigkeit. Der Task im Terminal für den Fingerprint löst, falls im Setup definiert, eine Eingabekette oder eine Zutrittsprüfung aus.

Verifikation mit Datenhaltung der Fingertemplates auf einem Transponder

Das Terminal pollt regelmäßig den Transponderleser, ob ein Transponder vorgehalten wurde. Wenn ja, wird die Seriennummer oder ein Speicherbereich des Transponders und die im Transponder gespeicherten Fingerdaten an den Fingerprint übergeben. Dieser wartet dann auf das Einlesen (Scannen) eines Fingers. Nach dem Einlesen (Scannen) des Fingers wird geprüft, ob der vom Ausweis übergebene Finger mit dem eingelesenem (eingescannten) übereinstimmt. Der Fingerprint übergibt an das Terminal PID und die Gültigkeit. Der Task im Terminal für den Fingerprint löst, falls im Setup definiert, eine Eingabekette oder eine Zutrittsprüfung aus.

5.14.5. Ablaufvarianten

Einlernen bei Identifikation / Verifikation mit Datenhaltung im Fingerprint Modul

- 1.) PID ermitteln (von Ausweis lesen oder über Listenauswahl)
- 2.) Finger scannen (Fingereigenschaften ermitteln)
- 3.) Einlernen (PID und Fingereigenschaften zusammenführen und im Fingerprint Modul speichern)

bzw.

- 1.) Finger scannen
- 2.) PID ermitteln
- 3.) Einlernen des Fingerprint Moduls

Einlernen bei Verifikation mit Datenhaltung auf einer Mifare-Karte

- 1.) PID ermitteln (von Ausweis lesen oder über Listenauswahl)
- 2.) Finger scannen (Fingereigenschaften ermitteln)
- 3.) Einlernen (PID und Fingereigenschaften zusammenführen und auf Mifare-Karte speichern)

bzw.

- 1.) Finger scannen
- 2.) PID ermitteln
- 3.) Einlernen und auf Mifare Karte speichern

Identifikation über Fingerprint Modul

- 1.) Finger scannen
- 2.) Identifikation über Fingerprint Modul

Verifikation über BIO-Key

- 1.) PID ermitteln (von Ausweis lesen)
- 2.) Finger scannen
- 3.) Verifikation über Fingerprint Modul bzw.
 - 1.) Finger scannen
 - 2.) PID ermitteln (von Ausweis lesen)
 - 3.) Verifikation über Fingerprint Modul

Verifikation über Mifare Karte

- 1.) Template von der Mifare Karte lesen
- 2.) PID ermitteln (von Ausweis lesen)
- 3.) Finger scannen
- 4.) Verifikation durch Fingerprint Modul

bzw.

- 1.) Finger scannen
- 2.) Template von der Mifare Karte lesen
- 3.) PID ermitteln (von Ausweis lesen)
- 4.) Verifikation durch Fingerprint Modul

Löschen eines Templates aus einem Fingerprint durch Identifikation

- 1.) Finger scannen
- 2.) Template aus Fingerprint Modul löschen bzw.
 - 1.) PID ermitteln (von Ausweis lesen oder über Listenauswahl)
 - 2.) Template aus Fingerprint Modul löschen

Löschen eines Templates aus einem Fingerprint durch Verifikation

- 1.) PID ermitteln (von Ausweis lesen oder über Listenauswahl)
- 2.) Finger scannen
- 3.) Template aus Fingerprint Modul löschen bzw.
 - 1.) Finger scannen
 - 2.) PID ermitteln (von Ausweis lesen oder über Listenauswahl)
 - 3.) Template aus Fingerprint Modul löschen

Löschen eines Templates von einer Mifare Karte

- 1.) Mifare Karte lesen
- 2.) Template von einer Mifare Karte löschen



Hinweis:

Ausführliche Anleitung zu den Einstellmöglichkeiten, finden Sie im Handbuch DatafoxStudioIV, in dem Kapitel „Funktionen im Setup>Fingerprint“.

5.14.6. Technische Daten Fingerprint-Modul

- ATMEL FingerChip
- ATMEL ARM9 Controller
- Speicherkapazität von 2000 Fingern
- Stromverbrauch ca. 120 mA bei 3,3 Volt, Sleep 1 uA
- Temperatur -20 bis + 85 °C
- Template: Idencom Kompakt Format 216 Byte
- Einlernzeit ca. 1,2 Sekunden + Prozesszeit Terminal
- Vergleichszeit: 0,014 Sekunden
- False Rejection Rate (FRR): $1,4 \times 10^{-2}$
- False Acceptance Rate (FAR) $1,0 \times 10^{-4}$
- Ab 100 Fingerabdrücken ist nur noch die Verifikation zu empfehlen. Kombination mit PIN per Tastatur o. Ausweis.
- Die Praxis zeigt, nicht bei allen Mitarbeitern können die Finger mit ausreichender Qualität erfasst werden.
- Abhängig vom Zustand der Finger. Bei diesen Personen muss dann mit Ausweis oder PIN erfasst werden.

5.15. Fingerprint, Informationen und Vergleich

Die Fingerprinttechnologie dient zur Erkennung von Personen anhand ihres Fingerabdrucks. Fingerprint ist die gängigste biometrische Identifikationsmethode. Verfügbar ist die Technologie in allen Datafox Terminals und in den Industrie-PCs.

Datafox verwendet zwei verschiedene Fingerprintverfahren. Beim optischen Sensor wird der Finger flach auf den Sensor gelegt und wieder heruntergenommen, wenn die Erkennung abgeschlossen wurde.

Beim Zeilensensor muss der Finger gleichmäßig vom Beginn des vordersten Fingerglieds gerade nach unten gezogen werden.
Die Templates der beiden Verfahren unterscheiden sich und können daher nicht gemeinsam genutzt werden.

Vorteile

Die Buchung des Fingerprints ersetzt das Lesen des Ausweises bzw. die Eingabe einer PIN. Fingerprint ist eine Alternative oder Ergänzung zu Transponder oder PIN, die sowohl Verwaltungsaufwand als auch Kosten spart. Es entfallen nicht nur die einmaligen Anschaffungskosten für Transponder, sondern auch Folgekosten für verloren gegangene, gestohlene oder nicht zurückgegebene Ausweise. Auch das Zuweisen und Verwalten der Transpondernummern entfällt, was sich vor allem bei z.B. saisonbedingt hoher Mitarbeiterfluktuation positiv bemerkbar macht. Außerdem können Transponder vergessen werden, was zu nachträglichem Aufwand bei der Datenpflege führt. Auch Manipulation wie z.B. das Buchen für einen anderen Mitarbeiter, ist ausgeschlossen.

Technische Informationen Technical information



[Produktvideo](#)
[Datafox Flächensensor](#)



[Produktvideo](#)
[Datafox Zeilensensor](#)

	Flächensensor area sensor	Zeilensensor line sensor
Max. Anzahl Templates im Modul	5000	2000
Größe Fingertemplate	635 Byte + 16 Byte Overhead	161, 216, 561 Byte + 16 Byte Overhead
Abnutzung Sensor durch Abrieb (abhg. von Schmutz u. Umgebung)	--	200.000 – 4.000.000 scans
RFID-Verfahren für Templates	Mifare Desfire (Application > 650 Byte / Finger notwendig/necessary)	Mifare Classic
Erkennungszeit bei 100 / 1000 Templates	< 1s / < 1s	< 1s / < 7s

Fingerprintverfahren

Alle Fingerprintverfahren vergleichen einen Fingerabdruck mit einem zuvor gespeicherten Abdruck. Das Abspeichern dieser Referenz-Fingerabdrücke nennt man Einlernen.

Identifikation

Der Sensor erkennt die Person anhand des Fingerabdrucks aus einer Liste angelernter Personen, die als Templates im Fingerprintmodul hinterlegt sind.

Verifikation, Templates im Modul

Dem Fingerprintsensor wird vor dem Scannen mitgeteilt, welche Person erwartet wird. Dann wird nur noch überprüft, ob der Fingerabdruck mit dieser ausgewählten Person übereinstimmt. Die Auswahl kann durch eine Liste, PIN oder RFID erfolgen.

Verifikation, Templates auf RFID-Ausweis

Die Verifikation erfolgt ebenso, als wenn die Templates im Modul gespeichert sind, allerdings wird das Template zuvor vom RFID-Ausweis gelesen. Auf einem Ausweis können ein oder zwei Templates gespeichert werden. Das Lesen der Templates benötigt je nach Größe und Anzahl Zeit, in der der Ausweis vor dem Leser verbleiben muss.

Fingertemplates – Was wird gespeichert?

Es werden nur Fingerprinttemplates gespeichert und keine echten Abbilder der Finger. Ein solches Template enthält nur mathematische Daten. Dieser Datensatz wird aus den sogenannten Minutien (Kreuzungspunkte der Fingerlinien) erstellt, mit dem keine Rekonstruktion des biologischen Fingerabdruckes möglich ist.



Empfehlung

Das Identifikationsverfahren ist für bis zu 100 Mitarbeitern einsetzbar. Bei höherer Mitarbeiterzahl sollte das Verifikationsverfahren eingesetzt werden.

Hinweise Datenschutz

Die Systeme speichern immer nur errechnete, komprimierte Daten. Die Fingerabdrücke können aus diesen Daten nicht wieder hergestellt werden. Beide Systeme erfüllen die Standards ISO-19794-4 und ANSI-378.

Hinweise Handhabung

- Feuchte Finger oder ein feuchter Sensor können das Ergebnis der Erkennung verschlechtern.
- Kalte und sehr trockene Finger können Schwierigkeiten bereiten. Durch kurzes Reiben des Fingers an einem anderen Finger kann das Verhalten deutlich verbessern.

Nicht alle Finger aller Personen eignen sich für Fingerprinter-kennung. Ein anderer Finger bringt häufig bessere Ergebnisse.

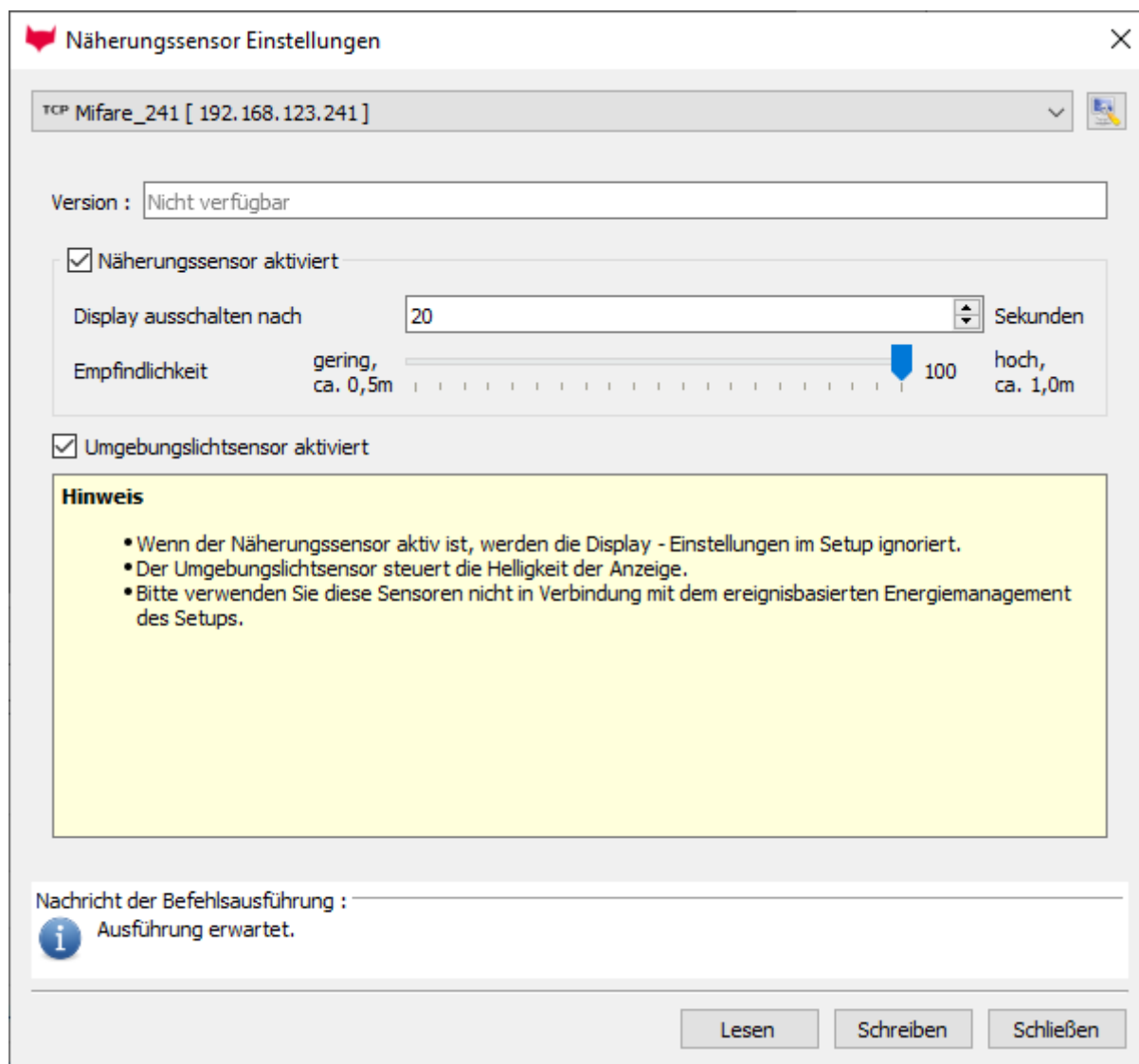
5.16. Weitere Funktionen

5.16.1. Einstellung Näherungs- & Umgebungslicht-Sensor im Studio

Folgende Parameter des Näherungs- und Umgebungslichtsensors sind ansteuerbar:

- „Näherungssensor“ ein- / ausschaltet;
- „Empfindlichkeit“ des Näherungssensors von 0% (~0,5Meter) bis 100% (~1,2Meter);
- „Display aus nach“ der letzten Erkennung des Näherungssensors (von 10 bis 65534 Sec.);
- „Umgebungslichtsensor“ ein- / ausschaltet.

Biosmenü der Geräte lassen sich die Einstellungen ebenso vornehmen wie im DatafoxStudioIV:



Näherungssensor Einstellungen

TCP Mifare_241 [192.168.123.241]

Version : Nicht verfügbar

Näherungssensor aktiviert

Display ausschalten nach 20 Sekunden

Empfindlichkeit gering, ca. 0,5m 100 hoch, ca. 1,0m

Umgebungslichtsensor aktiviert

Hinweis

- Wenn der Näherungssensor aktiv ist, werden die Display - Einstellungen im Setup ignoriert.
- Der Umgebungslichtsensor steuert die Helligkeit der Anzeige.
- Bitte verwenden Sie diese Sensoren nicht in Verbindung mit dem ereignisbasierten Energiemanagement des Setups.

Nachricht der Befehlsausführung :
 i Ausführung erwartet.

Lesen Schreiben Schließen

6. Technische Daten EVO 2.8 /3.5 /5.0 Pure

EVO 2.8 Pure Terminal V4.X

Gehäuse	Aufbau, Abmessungen (B x H x T)	Kunststoff: ABS // 109 mm x 200 mm x 85 mm				
	Gewicht (ohne Netzteil)	Basisgerät 0,35 KG zzgl. Wandhalterungsblech 0,125 KG				
System	Uhr	Echtzeituhr				
Daten-Speicher	Flash / Speichererweiterung (optional)	4 MB (optional 16 MB), 100.000 Schreibzyklen / SD-Card; max.2 GB				
Display	LCD	EVO 2.8	TFT: 320 x 240 Pixel, active area 57,6 x 43,2 mm mit LED-Backlight			
		EVO 3.5	TFT: 480 x 320 Pixel, active area 73,4 x 49,0 mm mit LED-Backlight			
		EVO 5.0	TFT: 800 x 480 Pixel, active area 108 x 64,8 mm mit LED-Backlight			
Tasten	Art, Größe	EVO 2.8	Tastatur über Touch-Display, Touchfläche 57,6 x 43,2mm, Lebensdauer nach Herstellerangabe: 1 Mio. Betätigungen			
		EVO 3.5	Kapazitives Touch-Display, Touchfläche 73,4 x 49,0mm, Touch verschleißfrei			
		EVO 5.0	Kapazitives Touch-Display, Touchfläche 108 x 64,8mm, Touch verschleißfrei			
Sensoren (nur EVO 3.5 / 5.0 Pure)	Näherungssensor	Aktivieren des Geräts bei Näherung eines Bedieners, Abstand ca. 0,8m				
	Helligkeitssensor	Reduzieren der Displayhelligkeit bei dunkler Umgebung				
Stromversorgung	Netzteil	12 V Gleichspannung				
	Leistungsaufnahme	Basisgerät 3 Watt, je nach Ausstattung bis max. 10 W				
	Uhr / RAM Pufferung	Goldcap, Sicherung der Uhrzeit bis zu einer Woche				
Umgebungswerte	Umgebungstemperatur	-20°C bis +60 °C (PoE -20°C bis +50°C)				
	Schutzart	IP 54				
Software	Konfigurationsprogramm	Setupprogramm (Datafox-Studio) zum Konfigurieren ohne Programmieraufwand				
	Kommunikationstools	http(S), Bibliothek (DLL, so) oder C++ Source-Code zur Einbindung in die Anwendung				
Modulerweiterungen	Für die Erweiterung um verschiedenste Funktionen wie Kommunikation, Ein- /Ausgänge, Sensoren,... stehen 5 Erweiterungsplätze für Module zur Verfügung.					
Datenübertragung zu PC/Server	USB	Micro-USB integriert				
	TCP/IP (optional)	TCP/IP-Betrieb mit integriertem TCP/IP-Stack, 10/100 Mbit				
	WLAN (optional)	wireless LAN Modul integriert, WLAN 802.11 bg und 802.11 n (nur 2,4GHz, ab 03/2021 auch 5GHz)				
	Mobilfunk (optional)	online über Mobilfunk-Modul 2G, 3G oder 4G				
	RS485 (optional)	RS485 Bus				
	USB-Host (optional)	für Datenübertragung per USB-Stick, Schutzklasse IP22				
	Bluetooth (optional)	Bluetooth Modul integriert; Reichweite bis max. 100 m				
Lesegeräteanschluss	RS232 extern (optional) (ML01-RS232)	Anschluss von Barcodeleser, Magnetkartenleser etc. über Mini-DIN Stecker				
Zutritt-Optionen	RS485 extern (ML01-RS485)	Anschluss von bis zu 3 Bussen mit insg. Bis zu 16 externen Türmodulen / Zutrittslesern				
	Türöffner-Relais mit Türüberwach. (ML01-DR1)	1 Relais Wechsler, 30V AC, 30V DC, 2A, max. 60 W; 1 dig. Eingang (galv. Getr.) für Türüberwachung				
MDE-Optionen	Modul digitale Eingänge (ML01-D01)	4 x digitaler Eingang, galv. Getrennt, bis 100kHz, sonst 250Hz, Low 0,0...1,5V; High 3,5...30,0V				
	Modul Relais Ausgänge (ML01-R01)	1 x Schließer, 1 x Wechsler, 30 V AC, 30 V DC, 2 A, max. 60 W				
	Modul analoge Eingänge Spannung (ML01-A1) / Strom (ML01-A2)	4 x Eingang, Auflösung 15 Bit, Genauigkeit ±2 %, Messbereiche 0-10 V / 0-25mA, andere Messbereiche und Funktionsisolierung 230 V auf Anfrage				
	Modul digitale Ausgänge Transistor (ML01-T1)	4x Ausgang	pro Aus-gang	pro Modul	pro Gerät, 40°C	pro Gerät, 60°C
		Aktiv 12V:	max. 0,8A	max. 0,8A	max. 1,4A	max. 1,0A
	Aktiv GND: (< 30V)	max. 1,4A	max. 2,0A	max. 4,0A	max. 2,0A	
Weitere Optionen	Fingerprint	Fingerprint Modul integriert; Sensor unten rechts				
	Transponderleser integriert	125kHz, z.B. Unique, Titan, Hitag, 13,56MHz, z.B. Legic, Mifare, ISO14443, ISO15693, SimonsVoss, iButton, Nedap				
	GPS-Empfänger / Receiver	50 Channels, GPS L1 frequency C/A, GALILEO Open Service L1				
	Barcodescanner integriert	1D oder 2D/QR Scanner integriert				
	Säule	Säule für freies Aufstellen				
	Fieberkontrolle am Handgelenk	Einsatz nur bei Raumtemperatur +15 - +35°C, kein Wind, keine direkte Sonne. Seitlich am Gerät montiert.				

6.1. Module Kommunikation

LAN (TCP/IP)	Breite 20mm	10/100MBit, IPv4, IPv6
WLAN	Breite 20mm	Standard 802.11.b/g, Verschlüsselung WEP, WPA2 802/11i
GPRS	Breite 40mm	GPRS class 10, Quadband, Mini-SIM Fassung
RS485	Breite 20mm	RS485-Vernetzung, bis zu 30 Teilnehmer

6.2. Module Zutritt

RS485	Breite 20mm	RS485 Anschluss für die Zutrittsleser, Relaismodule,... Spannungsversorgung von 1 externen Leser bei Verwendung der Datafox Netzteile mit 12V; max. 350 mA out
ZK-IO	Breite 20mm	1 Relais Wechsler, 30 V AC, 30 V DC, 2 A, max. 60 W; 1 digitaler Eingang für Türüberwachung,...

6.3. Module I/O (MDE)

Digitale Eingänge ML01-D1	Breite 20mm	4 x digitaler Eingang, Funktionsisolierung 230V, je nach Gerätetyp bis zu 250kHz Low 0,0...1,0V; High 3,5...30,0V															
Digitale Ausgänge Relais ML01-R1	Breite 20mm	1 x Schließer, 1 x Wechsler, 30 V AC, 30 V DC, 2 A, max. 60 W															
ML01-DR1	Breite 20mm	1 Relais Wechsler, 30 V AC, 30 V DC, 2 A, max. 60 W; 1 digitaler Eingang (galv. getrennt) für Türüberwachung,...															
Digitale Ausgänge Transistor ML01-T1	Breite 20mm	4 x Transistorausgang, aktiv 12V oder aktiv GND, weitere Details siehe Infoblatt															
		<table border="1"> <thead> <tr> <th></th> <th>pro Ausgang</th> <th>pro Modul</th> <th>pro Gerät, 40°C</th> <th>pro Gerät, 60°C</th> </tr> </thead> <tbody> <tr> <td>Aktiv 12V:</td> <td>max. 0,8A</td> <td>max. 0,8A</td> <td>max. 1,4A</td> <td>max. 0,8A</td> </tr> <tr> <td>Aktiv GND: (max. 30V)</td> <td>max. 0,8A</td> <td>max. 2,0A</td> <td>max. 10,0A</td> <td>max. 2,4A</td> </tr> </tbody> </table>		pro Ausgang	pro Modul	pro Gerät, 40°C	pro Gerät, 60°C	Aktiv 12V:	max. 0,8A	max. 0,8A	max. 1,4A	max. 0,8A	Aktiv GND: (max. 30V)	max. 0,8A	max. 2,0A	max. 10,0A	max. 2,4A
	pro Ausgang	pro Modul	pro Gerät, 40°C	pro Gerät, 60°C													
Aktiv 12V:	max. 0,8A	max. 0,8A	max. 1,4A	max. 0,8A													
Aktiv GND: (max. 30V)	max. 0,8A	max. 2,0A	max. 10,0A	max. 2,4A													
Analoge Eingänge Spannung ML01-A1	Breite 20mm	4 x Eingang, Auflösung 15 Bit, Genauigkeit ± 2 %, Messbereich 0-10 V, andere Messbereiche und Funktionsisolierung 230 V auf Anfrage															
Analoge Eingänge Strom ML01-A2	Breite 20mm	4 x Eingang; Auflösung 15 Bit, Genauigkeit ± 2 %, Messbereiche 0-25 mA; Funktionsisolierung 230 V auf Anfrage															
Analoge Ausgänge	Breite 20mm	In Vorbereitung															

6.4. Module verschieden

RS232-Modul	Breite 20mm	RS232 Schnittstelle mit MiniDIN-Buchse oder Federklemme, 5V-Ausgang max. 0,5A, bei USB-Versorgung max. 100mA.
GPS	Breite 20mm	50 Channels, GPS L1 frequency C/A, GALILEO Open Service L1
Micro-SD Card	Breite 20mm	Micro-SD Karte max. 2GB, je nach Einbauort von außen zugänglich
Mobil-Box-Modul	Breite 40mm	Zentralanschluss für Spannungsversorgung, (8-30V DC), 1 Relais, 2 digitale Eingänge und Anschluss für Mobil-Dockingstation mit Timeboy
Beschleunigungssensor	Breite 20mm	3D-Beschleunigungssensor In Vorbereitung

7. FAQ & Fragen und Antworten

Eine umfangreiche Sammlung von FAQ finden Sie auf unserer Homepage:

<http://www.datafox.de/faq-de.html>

8. Index

A

analoge Eingänge 47

B

Barcodescanner 168
Bilder 30
Bios 21

D

Data on Card 163
DHCP 21, 65
Digitale Eingänge 48
DIP-Schalter ZK 111
DNS 65

E

EMA 130, 134
Entsorgung 10
EVO 82

F

Falscher 114
FAQ 189
Feiertagssteuerung ZK 76
Fingerscanner Zeilensensor 178
Fingersensor Optisch 170

G

GPRS 70
Grafiken im Display 28

I

Inbetriebnahme 18
Installationsvoraussetzungen 12

K

Kommunikation 51
Umschalten 51

L

Lautstärke 21
Leitungslänge 116
Berechnung für ZK 116

M

Mobilfunk Verbindung Status 71

N

Näherungssensor 187

O

Office-Mode 156, 158
Office-Mode-1 156
Office-Mode-2 158
Online Zutritt 121

P

PHG 93

R

Reinigung 8
Relais 48
RFID 162

S

Schleusenfunktion 105
Schutzart 6
SMS 72
Spannungsversorgung 39
POE 39

T

TCP/IP 58, 161
Temperaturbereich 7
Touchkalibrierung 21

U

Umgebungslichtsensor 187
USB 51, 53
USV 13

W

WLAN 61, 62, 63

Z

Zeitsteuerung 76
Zutritt 50
Anschluss 50
Leitungsquerschnitt 116
Statusmeldungen 129
Tabellenbeschreibung 79
Zutritt mit PHG 95
Zutrittskontrolle 76, 138