



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

Handbuch ZK-MasterIV

Flexible Datenerfassung mit Methode



© 2017 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
23.04.2012	Alle	Überarbeitung des Handbuchs auf Versionstand 04.02.02.xx
30.04.2012	ZK-PHG	Schaltpläne hinzugefügt
10.09.2012	Alle	Anpassung auf SW 04.02.03
23.05.2013	Alle	Anpassung auf SW 04.02.04
06.11.2013	ZK	Online über HTTP, Leser PHG-E-Serie
04.09.2015	Alle	Anpassung auf FW 04.02.05 und DatafoxStudioIV 0.03.05.06
09.11.2017	POE Hinweise	POE Hinweise

Versionsänderungen

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

Produkt- bezeichnung	XX. Geräte- generation	YY. Kompatibilität (welche Versionen können zusammen einge- setzt werden)	ZZ. Versionsnummer (Funktionser- weiterung)	Build Fehlerbeseitigung (mit einer neuen Version wird die Build-Nr. auf Null gesetzt)
z. B. ZK-MasterIV	04.	02.	01.	04

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

Firmware, Studio und DLL Gültigkeit

Firmware: 4.02.05.xx.

Studio: 4.03.06.xx

Dll: 4.03.05.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 Handbuches	2
2.2.	Einschränkung der Gewährleistung	2
2.3.	Typografie des Handbuches	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
3.3.1.	Temperatur	5
3.4.	Reparatur	5
3.5.	Reinigung	5
3.6.	Sonstige Hinweise	5
3.7.	Entsorgung	6
4.	Systemvoraussetzungen / Hardware	7
4.1.	Systemaufbau	7
4.2.	Voraussetzungen für den Betrieb der Datafox-Geräte	7
4.3.	Kompatibilität	8
4.3.1.	Das Firmwaredateiarchiv (*.dfz)	8
4.3.2.	Datafox-Geräte und Geräte-Firmware	8
4.3.3.	Geräte-Firmware und Geräte-Setup	9
4.3.4.	Geräte-Firmware und Kommunikations-DLL	9
4.3.5.	Kommunikations-DLL und DatafoxStudioIV	9
4.3.6.	DatafoxStudioIV und Geräte-Setup	9
4.3.7.	Update / Downgrade	10
5.	Gerät	11
5.1.	Inbetriebnahme ZK-MasterIV	11
5.2.	Leitfaden zur Inbetriebnahme für Geräte ohne Display	12
5.2.1.	Einrichtung des ZK-MasterIV	12
5.2.2.	Installation des ZK-MasterIV	12
5.2.3.	Fehlersuche bei der Inbetriebnahme des ZK-MasterIV	12
5.3.	Bedienung des Gerätes	13
5.3.1.	Zugang zum Bios-Menü	13
5.3.2.	LED-Statusanzeige	15
5.4.	Montage der Boxengeräte	16
5.5.	Spannungsversorgung ZK-MasterIV	17
5.5.1.	Spannungsversorgung mit Netzteil	17
5.5.2.	Spannungsversorgung über POE-Adapter	17
5.6.	Anschluss	18
5.6.1.	Steckerbelegung	18
5.6.2.	Spannungsversorgung	19
5.6.3.	Digitale Eingänge	19

5.6.4.	Digitale Ausgänge	20
5.7.	Kommunikationsarten	21
5.7.1.	Kommunikation über RS232.....	21
5.7.2.	Übergang von RS232 auf RS485	22
5.7.3.	Kommunikation RS 485.....	23
5.7.4.	Kommunikation über TCP/IP	24
5.7.4.1.	Einstellung der IP-Adresse	25
5.7.4.2.	Versenden von Datensätzen mit HTTP über LAN / WLAN	26
5.7.4.3.	Übergang von TCP/IP auf RS232 / RS485 über Comserver.....	27
5.7.4.4.	Einrichtung des Comserver Lantronix UDS 11	28
5.7.5.	Kommunikation über WLAN	30
5.7.6.	Kommunikation über USB	41
5.7.7.	Kommunikation über Modem.....	44
5.7.8.	Kommunikation über Mobilfunk (GSM bzw. GPRS/GSM).....	47
5.7.8.1.	Notwendige Einstellungen für die Kommunikation über das Mobilfunknetz	48
5.7.9.	Kommunikation per SMS.....	49
5.7.9.1.	SMS versenden.....	49
5.7.9.2.	SMS empfangen	50
5.8.	Anschluss der Zutrittskontrolle	52
5.8.1.	Zutrittskontrolle II mit PHG-Modulen.....	52
5.8.1.1.	Anschluss der PHG-Leser	53
5.8.1.2.	Konfiguration	59
5.8.2.	Zutrittskontrolle II mit TS-Lesern	61
5.8.2.1.	Aufbau und Installationsvarianten	62
5.8.2.2.	Anschluss der TS-Leser	68
5.8.3.	Beschreibung der Tabellen für die Zutrittskontrolle 2.....	75
5.8.4.	Onlinefunktionen der Zutrittskontrolle	77
5.8.4.1.	Online über HTTP-Anbindung	77
5.8.4.2.	Online über DLL-Anbindung.....	80
5.8.5.	Funktionserweiterung für die Zutrittskontrolle 2	81
5.8.5.1.	Allgemeine Informationen.....	81
5.8.5.2.	Beispiele	81
5.8.5.3.	Beschreibung der Tabelle „Action2“	85
5.8.6.	Statusmeldungen der Zutrittskontrolle	86
5.8.7.	Statusanzeige der Zutrittsmodule über LEDs	89
5.9.	Piepser	90
6.	Technische Daten ZK-MasterIV	91
6.1.	Technische Daten digitale Eingänge	91
6.2.	Technische Daten digitale Ausgänge	91
7.	FAQ	91
8.	Index	92

1. Zu Ihrer Sicherheit

Sicherheitshinweise für den Umgang mit den Datafox Produkten



Das Gerät 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!

Achtung!

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 +70° C
Mobilfunkmodem -20° C bis +55° C



In Bereichen, in welchen Handyverbot besteht, müssen GSM, 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 : 2006 + A1:2007
- EN 55024 : 2003
- EN 61000 – 6 – 2: 2005
- IEC 61000-3-2 : 2005 + A1:2008 + A2:2009
- IEC 61000-3-3 : 2008



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 „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 wird.

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	Ankürzung 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 die Funktionalität des ZK-MasterIV 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 ZK-

MasterIV 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 nur mit einer Stromquelle mit begrenzter Leistung, entsprechend EN 60950-1 betrieben werden.

Anschlussspannung der MasterIV-Geräte: 12 bis 24 Volt AC / 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.

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

3.3.1. Temperatur

Das ZK-MasterIV hat einen zugelassenen Temperaturbereich von – 20°C bis + 70°C.

Eine Heizung ist bei uns 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.

3.4. Reparatur

Die Datafox Geräte sind wartungsfrei und 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.

3.5. Reinigung

3.6. 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 für sie vorgesehenen Mitteln 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.

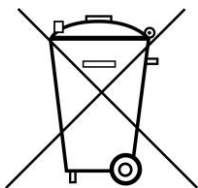
Um einen Missbrauch der SIM-Karte zu vermeiden, denken Sie bei Verlust oder Diebstahl des Gerätes daran, die SIM-Karte sofort sperren zu lassen.

3.7. 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).



Somit darf das Gerät 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

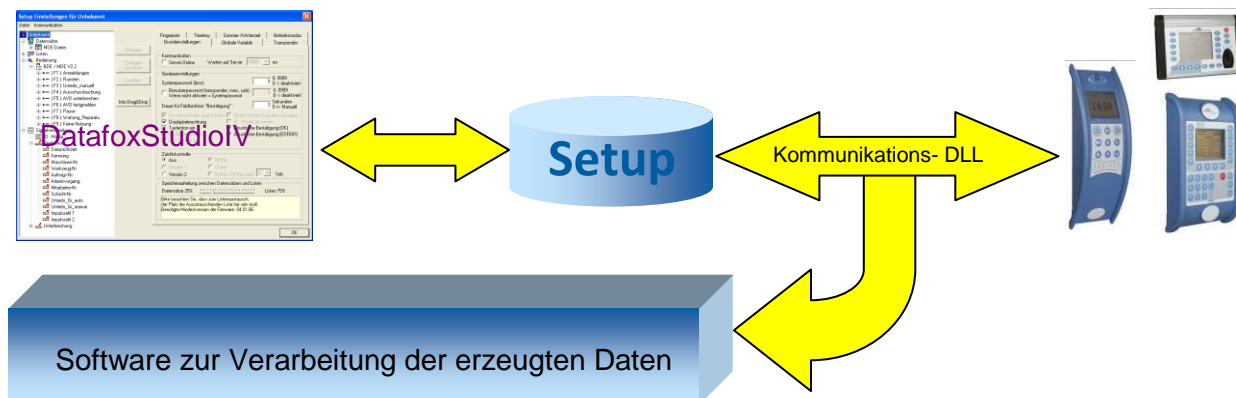
4.1. Systemaufbau

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

Setuperstellung

Setup speichern

Setup auf Gerät übertragen



4.2. Voraussetzungen für den Betrieb der Datafox-Geräte

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

Hauptkommunikation:

- RS232 per Modem > ein Serielles Null-Modem-Kabel mit D-Sub 9 polig Stecker-Buchse (siehe Anschluss analog Modem).
- WLAN > einen störungsfreien Funkkanal zu einem Access Point (802.11 b/g) in Reichweite (siehe Anschluss WLAN).
- GSM/GPRS > eine störungsfreie Mobilfunkverbindung (siehe Anschluss GSM).
- RS485 > eine dem EIA-485 Standard entsprechende Übertragungstrecke (siehe Anschluss RS485).
- USB > ein Standard USB Kabel (siehe Anschluss USB).
- TCP/IP > min. ein Standard Ethernet Kabel, kein „cross over“ (siehe Anschluss TCP).
- HTTP(Internet) über LAN > TCP/IP-Anschluss mit freiem Internetzugang. Die Daten werden dann an einen Server gesendet.



Hinweis:

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

4.3. 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

4.3.1. 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.

4.3.2. 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.

4.3.3. 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.

4.3.4. 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.

4.3.5. 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.

4.3.6. 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.

4.3.7. 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 ZK-MasterIV

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



Hinweis:

Bei Auslieferung steht die Hauptkommunikation auf RS232.



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 für Geräte ohne Display

5.2.1. Einrichtung des ZK-MasterIV

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



Achtung:

Das Einstellen der Schnittstelle für die Hauptkommunikation muss über das Programm DatafoxStudioIV erfolgen.

- ▶ Setup des Gerätes einspielen

Siehe Handbuch „DatafoxStudioIV“

5.2.2. Installation des ZK-MasterIV

- ▶ Montage des Gerätes am Bestimmungsort
- ▶ Anschlüsse herstellen für:
 - [Spannungsversorgung](#)
 - Zusatzmodule anschließen
 - [Zutrittsmodule TS-Serie](#)
 - [Zutrittsmodule PHG](#)
 - Kommunikation über Bios Menü in [DatafoxStudioIV](#) einstellen:
 - [RS232](#)
 - [RS485](#)
 - TCP / IP (HTTP)
 - Digitale Eingänge
 - Digitale Ausgänge
- ▶ Gerät fertig befestigen

5.2.3. Fehlersuche bei der Inbetriebnahme des ZK-MasterIV

- ▶ Als erstes schauen Sie bitte auf unserer Webseite auf die FAQ <http://www.datafox.de/faq-de.html>
- ▶ Kleine Tips:
 - 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 des Gerätes

5.3.1. Zugang zum Bios-Menü

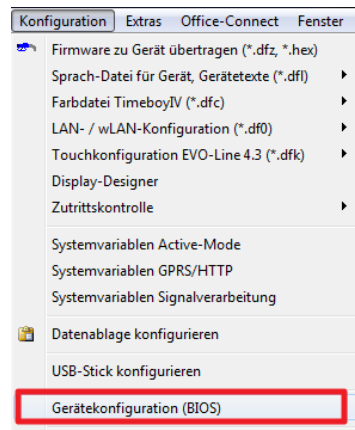


Achtung:

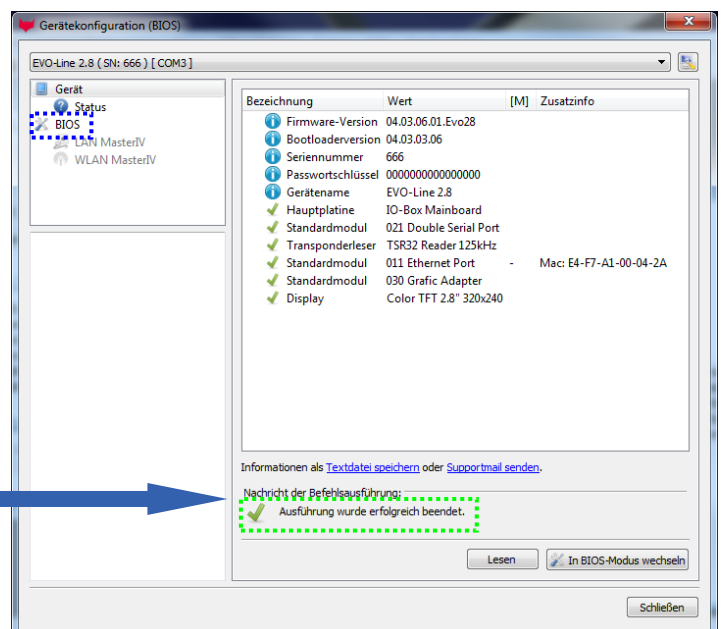
Da das Gerät kein Display besitzt, müssen die Einstellungen über das DatafoxStudioIV vorgenommen werden.

Öffnen Sie das DatafoxStudioIV und stellen Sie eine Verbindung über RS232 zum Gerät her.

Klicken Sie auf Konfiguration



Klicken Sie auf „Gerätekonfiguration (Bios)“



Klicken Sie auf „In Bios – Modus wechseln“

Nach erfolgreicher Aktivierung des Bios erhalten Sie diese Meldung.

Klicken Sie dann auf Bios

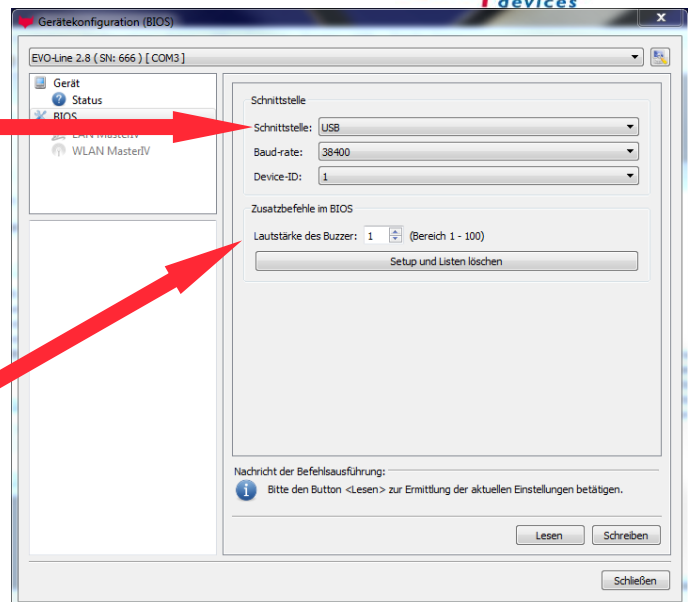


Achtung:

Ist die Hauptkommunikation des Gerätes nicht auf RS232 eingestellt, muss das Gerät bei einem Neustart „abgefangen“ werden. Bei einem Neustart wird die RS232 immer geprüft. Drücken Sie erst In Bios – Modus wechseln und dann schalten Sie das Gerät ein. Durch zwei kurze Pieptöne signalisiert das Gerät, dass das Bios aktiviert wurde.

Unter „Schnittstelle“ können Sie die Hauptkommunikation des Gerätes umstellen. Je nach der Ausstattung des Gerätes stehen hier die entsprechenden Schnittstellen zur Verfügung.

Die Lautstärke des Buzzers können Sie hier einstellen.



Achtung:

Alle Einstellungen die hier vorgenommen werden, werden erst nach einem Neustart des Gerätes übernommen.



Hinweis:

Zu weiteren Einstellungen z.B. W-Lan, TCP/IP oder GPRS nutzen Sie bitte das Handbuch DatafoxStudioIV.

5.3.2. LED-Statusanzeige

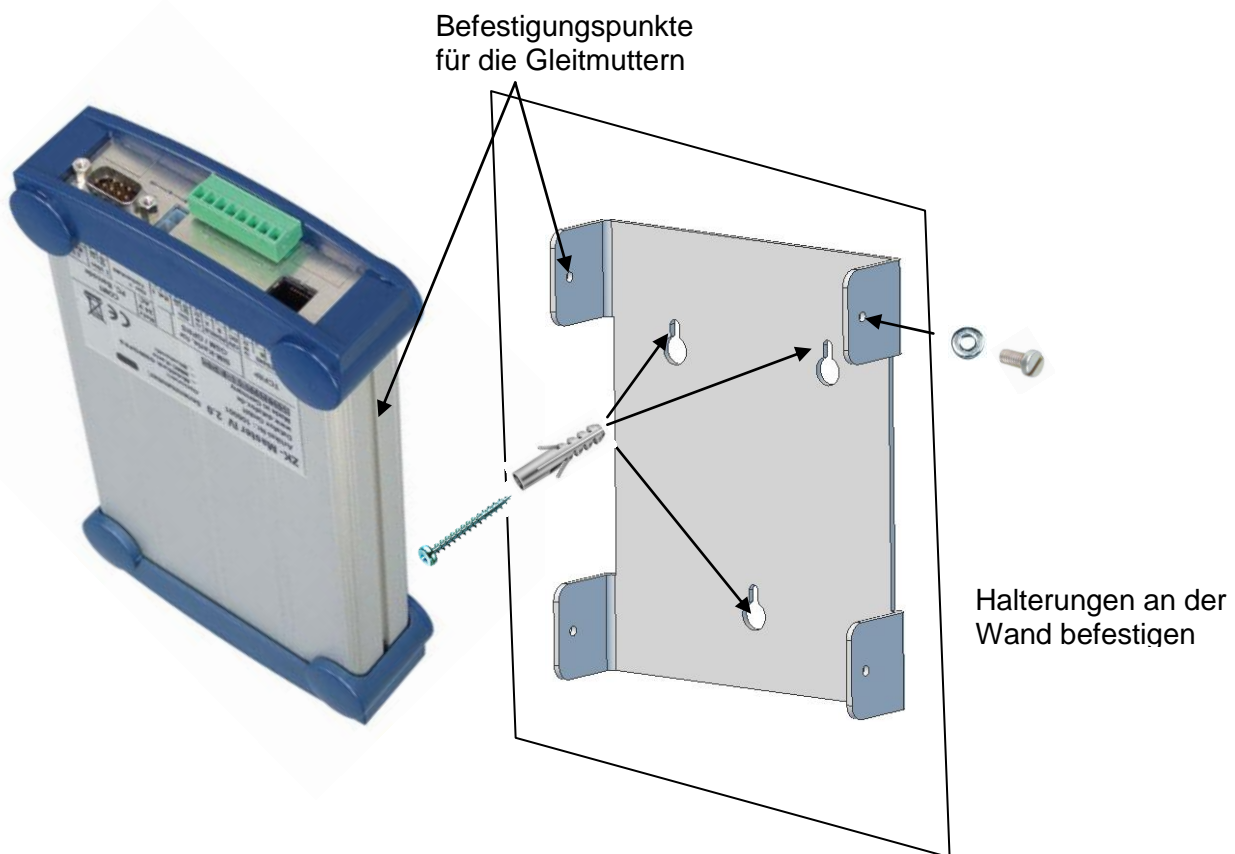
Durch die LED werden bestimmte Zustände des Gerätes, z.B. kein Setup vorhanden usw. und der GSM/GPRS Status einer Verbindung angezeigt.

Den Möglichkeiten der Signalisierung vom Zustand des Gerätes sind dabei natürlich Grenzen gesetzt. Dennoch werden eine ganze Menge an Zuständen signalisiert, was eine Analyse bei Fehlern wesentlich erleichtert.

ERROR	POWER	GSM/GPRS	Zustand des Gerätes
On	On	Off	Bootloader aktiviert
On	On	On	Start
Off	1 Hz	Off	Booten
1 Hz	1 Hz	Off	Kein Setup
1 Hz	On	unverändert	Bedienstopp
Off	On	unverändert	normaler Betrieb
1 Hz	On	unverändert	System Stop
Off	unverändert	Off	SIM-OK Offline
2 Hz	unverändert	aus 150ms ein 150 ms pause 1000ms	keine SIM
2 Hz	unverändert	aus 150ms ein 150 ms aus 150 ms ein 150ms pause 1000ms	keine SIM-PIN
2 Hz	unverändert	aus 150ms ein 150 ms aus 150ms ein 150ms aus 150ms ein 150ms pause 1000ms	keine SIM-PUK
2 Hz	unverändert	aus 150ms ein 150 ms	SIM-Fehler
unverändert	aus für 50ms je Datenpaket	unverändert	Kommunikation aktiv (Status)
Off	unverändert	ein 150ms aus 150 ms pause 4000ms	Verbindungsaufbau zum Provider
Off	unverändert	ein 150ms aus 150 ms ein 150ms aus 150 ms pause 4000ms	Verbindungsaufbau zum Server
Off	unverändert	ON	Online GPRS/GSM
ON	unverändert	unverändert	LOW VOLTAGE
Ca. 5 Hz	unverändert	unverändert	allgemeiner Fehler; nicht definiert

5.4. Montage der Boxengeräte

Um das Gerät an der Wand zu befestigen stehen 2 Wandalter zur Verfügung.



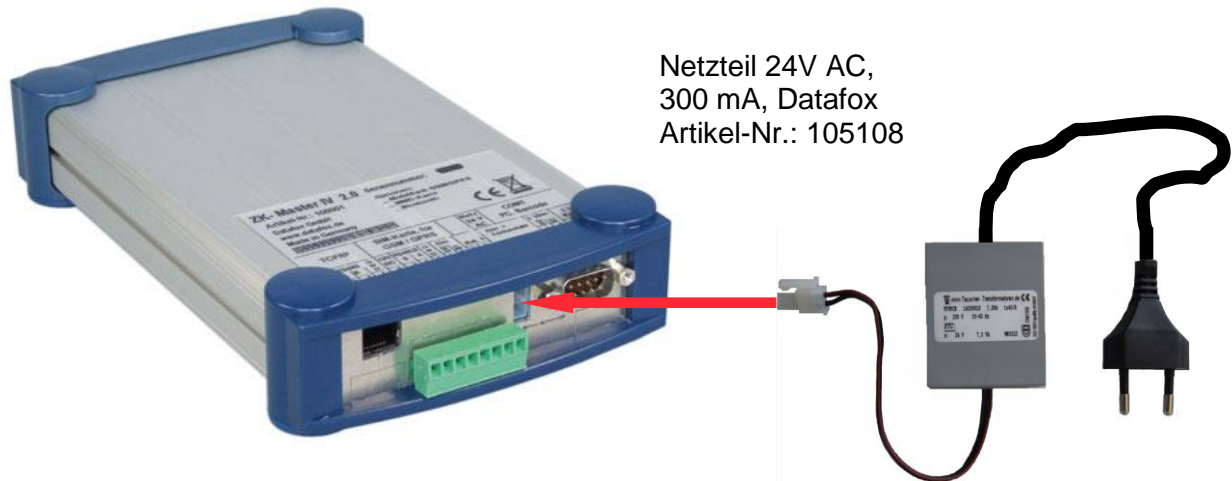
Im Lieferumfang des Wandhalters sind folgende Teile enthalten.

- ▶ Halblech
- ▶ 3 Dübel Ø5
- ▶ 3 Schrauben 3,5x30
- ▶ 4 Schrauben M4x8
- ▶ 4 Unterlegscheiben M4

5.5. Spannungsversorgung ZK-MasterIV

5.5.1. Spannungsversorgung mit Netzteil

Die Spannungsversorgung wird über ein Netzteil 230V /24V AC hergestellt.



Wenn für den Anschluss nur eine Schraubklemme zur Verfügung steht, schneiden Sie einfach den 230 Volt Stecker ab und schließen Sie die Adern an die Schraubklemme an.

5.5.2. Spannungsversorgung über POE-Adapter

Der POE-Adapter wird anstelle des Netzteils montiert.
Voraussetzung dafür ist eine Netzwerk mit Spannungsversorgung.
Der Standard des Adapters ist **PoE Standard 802.3af**.

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.

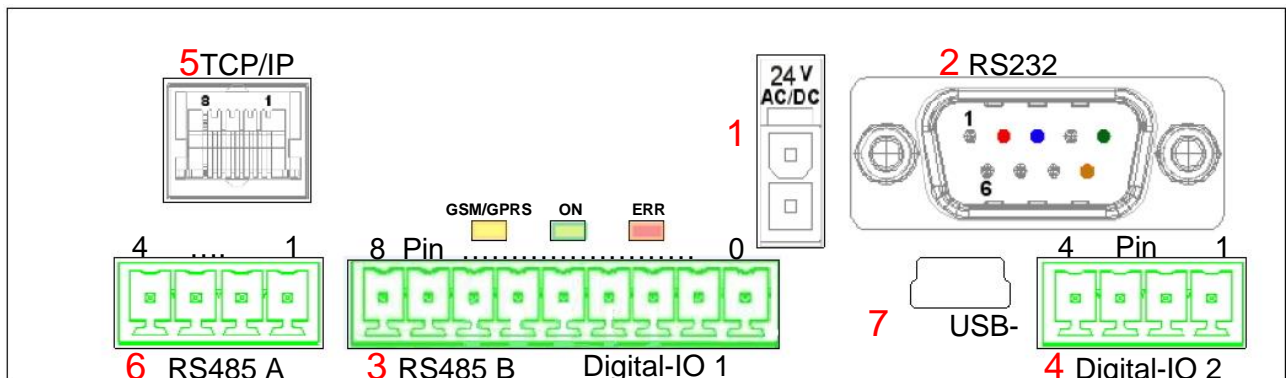


Achtung:

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.

5.6. Anschluss

5.6.1. Steckerbelegung



Steckerleiste des ZK-MasterIV Stecker 3=9pol ab HW3.x

Bezeichnung	Stecker	PIN	Beschreibung
Spannungsversorgung	1		24 V 300 mA AC/DC (Wird eine Gleichspannung angeschlossen, ist die Polung zu beachten.)
RS232 Schnittstelle D-Sub 9 polig	2	2	TxD
		3	RxD
		5	GND
Digitale Eingänge Relais 1	3	3	Eingang 5 kHz 0 - 2 Volt = logisch 0 (VILmax = 2,0 V) 5 - 30 Volt = logisch 1 (VIHmin = 5 V)
		4	GND
Digitale Eingänge Relais 2	4	3	Eingang 10 Hz 0 - 3 Volt = logisch 0 (VILmax = 3,0 V) 12-30 Volt = logisch 1 (VIHmin = 12,0 V)
		4	GND
Digitale Ausgänge	3	0	Normally-close (Öffner) ! 9pol, ab 05.2013 ist dieser Pin bei allen neuen Geräten hinzugekommen, für ältere Versionen gilt 8pol Belegung Pin 1-8
		1	common (max. 2,0 A bei 42 V AC bzw. 30 V DC)
	4	1	common (max. 2,0 A bei 42 V AC bzw. 30 V DC)
		2	Normally-open (Schließler)
TCP / IP	5		RJ 45
RS485 Schnittstelle für die Kommunikation mit PC	6	1	GND
		2	Datenkanal A
		3	Datenkanal B
		6	24 V DC
RS485 Schnittstelle der Zutrittskontrolle	3	5	GND
		6	Datenkanal A
		7	Datenkanal B
		8	12 V DC



Achtung:

Stecker 3 wurde von 8 pol. auf 9 pol. geändert. Achten Sie bei einem Austausch der Hardware darauf, dass Sie den 8pol. Stecker richtig in die 9pol Buchse stecken oder klemmen Sie auf den 9pol. Stecker um.

5.6.2. Spannungsversorgung

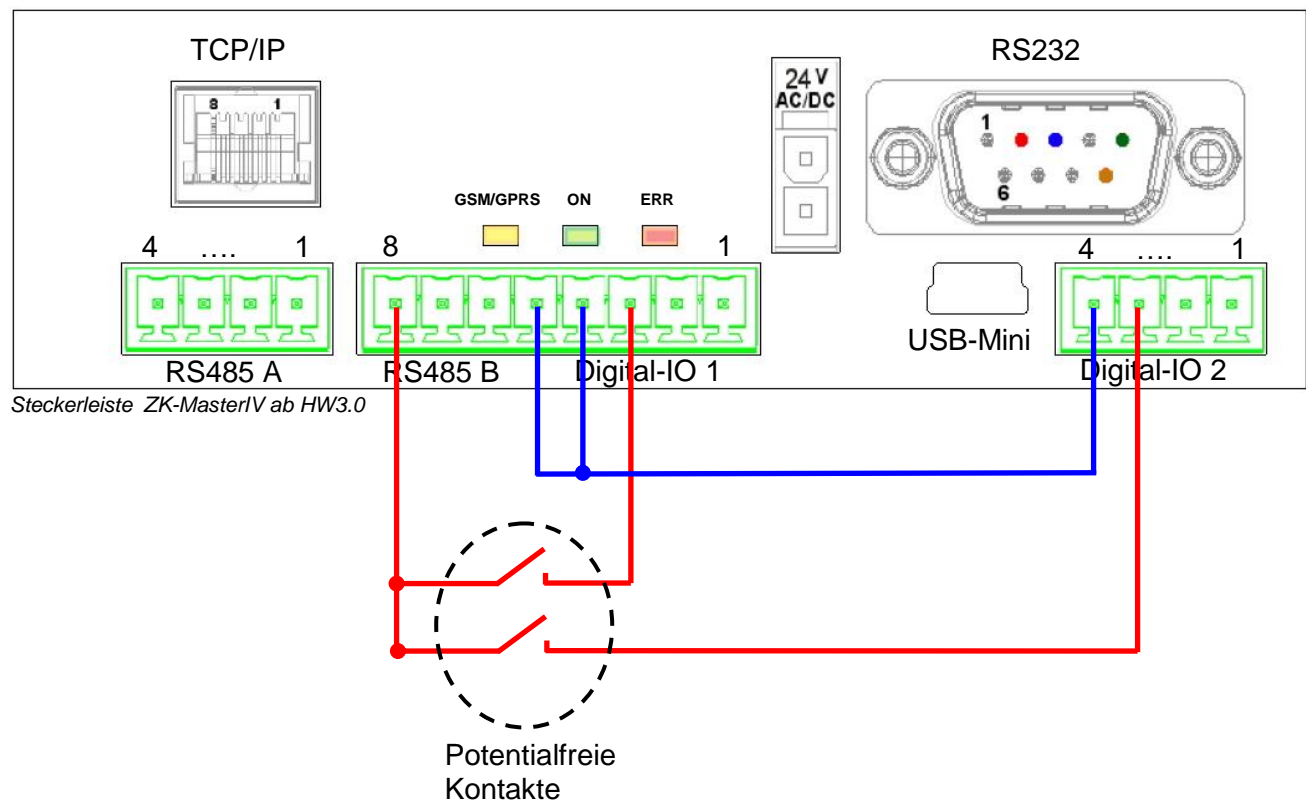
Achtung:
 Es darf grundsätzlich nur eine Spannungsquelle an den ZK-MasterIV angeschlossen werden. Hiefür ist ein 12 – 24 V 300 mA AC/DC Netzteil zu verwenden. Über dieses Netzteil darf max. ein externer Verbraucher (z. B. ein Transponderleser für die Zutrittskontrolle) über die RS485 Schnittstelle mit Spannung versorgt werden.

Siehe Kapitel „ Spannungsversorgung“.

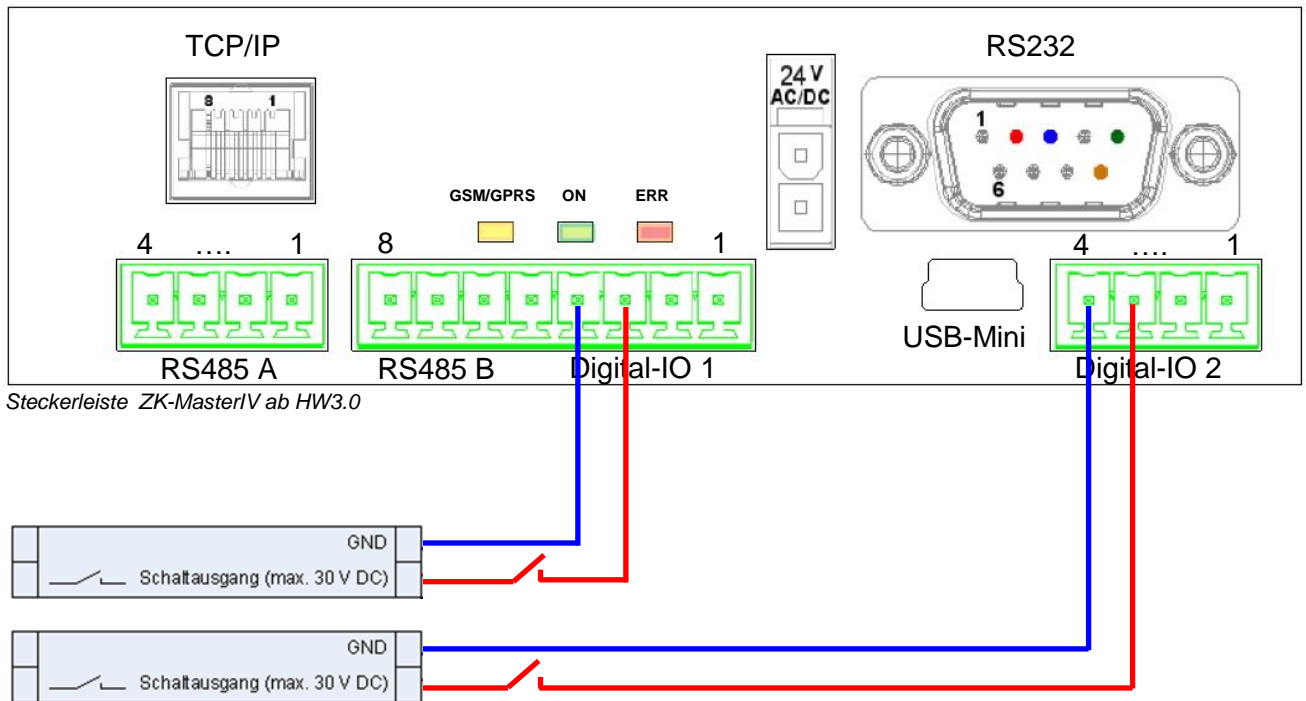
5.6.3. Digitale Eingänge

Achtung:
 Achten Sie in jedem Fall auf ordnungsgemäße Signale.

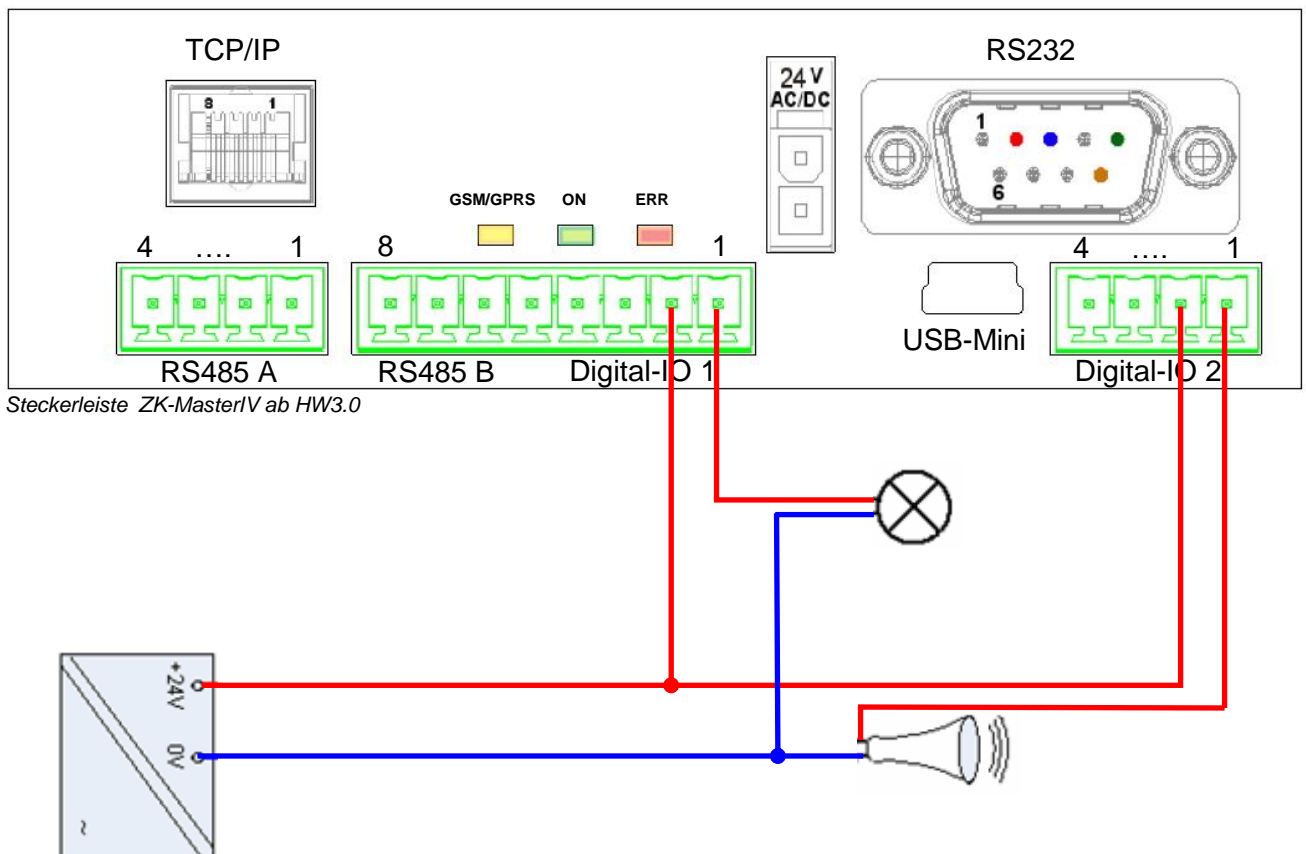
Nachfolgend sind zwei Anschlussbeispiele für die Nutzung der digitalen Eingänge mit dem ZK-MasterIV dargestellt. Die erste Abbildung zeigt den Anschluss von potentialfreien Schaltkontakten z. B. für eine Türüberwachung ohne externe Spannungsquelle.



In der folgenden Abbildung ist der Anschluss von potentialbehafteten Schaltkontakten dargestellt. Die max. Spannung von 30 V DC am Schaltausgang und somit am Digitalen Eingang des ZK-MasterIV ist zu beachten.



5.6.4. Digitale Ausgänge



5.7. Kommunikationsarten



Achtung:

Die Kommunikationsart des Gerätes ist abhängig von der Ausstattung des Gerätes. 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:

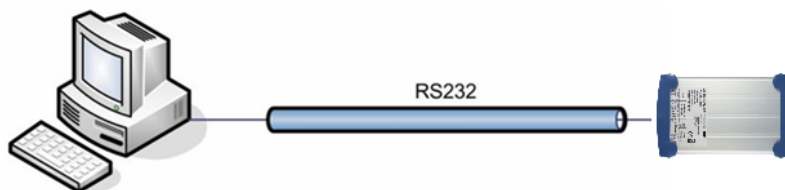
1. über Systemenü Bios am Gerät,
2. ab Firmware 04.02.04 im Setup mit der Feldfunktion „Kommunikation umschalten“ Mehr hierzu finden Sie im Handbuch [DatafoxStudioIV](#).

Mögliche Kommunikationsarten sind:

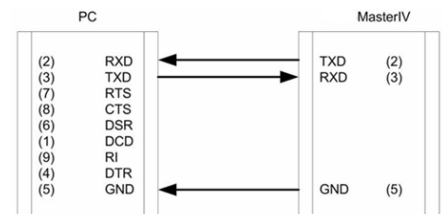
1. RS232
2. RS485
3. TCP/IP über LAN
4. TCP/IP über das Internet (per HTTP)
5. TCP/IP über WLAN
6. USB als Verbindung zum PC
7. USB mit Datentransfer auf Stick
8. GPRS Verbindung über das Mobilfunknetz
9. GSM Verbindung über Modem

5.7.1. Kommunikation über RS232

Um über RS232 mit einem Gerät kommunizieren zu können, muss das Gerät für diese Kommunikationsart im Systemenü-Bios eingestellt sein. Zusätzlich sind Baudrate und Timeout der RS232-Schnittstelle des Terminals und der RS232-Schnittstelle des PCs aufeinander abzustimmen. Als Baudrate sind zulässig 9600, 19200 sowie 38400. Der Timeout muss zwischen 100 und 2000 liegen. Standardmäßig wird der Timeout bei Auswahl der Kommunikationsart RS232 auf 100 gesetzt. Verwenden Sie zum Anschluss des ZK-MasterIV an einen PC eine RS232 Verbindungsleitung mit einer 1:1 Belegung, entsprechend Datafox Artikel-Nr. 20010.



Anschluss des ZK-MasterIV per RS232



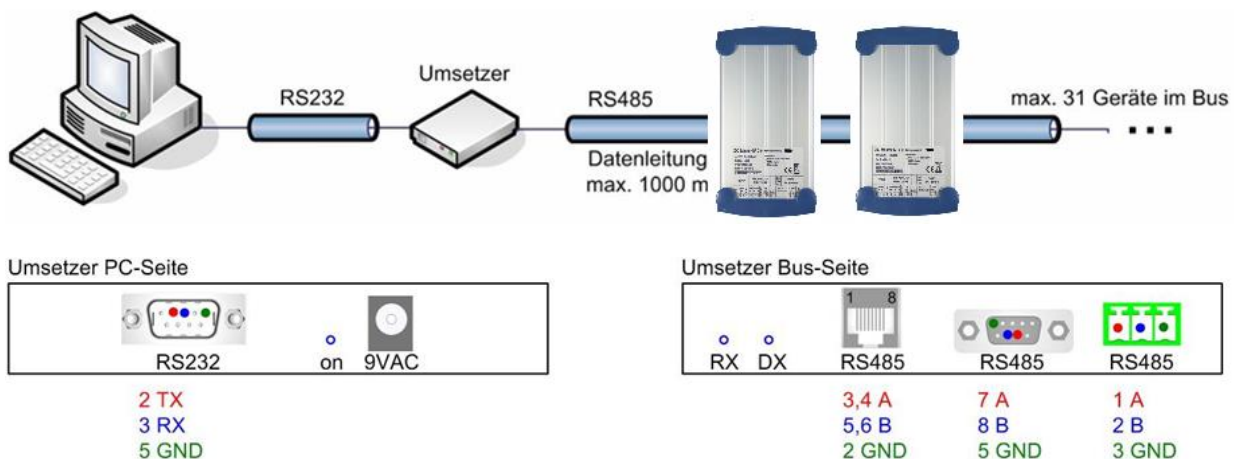
5.7.2. Übergang von RS232 auf RS485

Über einen Umsetzer von RS232 auf RS485 können bis zu 31 Geräte an eine serielle Schnittstelle eines PCs oder Servers angeschlossen werden. Die Geräte sind dabei über einen RS485 Bus verbunden. Die Stromversorgung kann über ein zentrales Netzteil mit entsprechender Leistung erfolgen. Hierbei ist abhängig von Leitungsquerschnitt und Leitungslänge der Spannungsabfall zu berücksichtigen. Die Anschlussbelegung für den Umsetzer wird am Beispiel des Datafox Umsetzers RS232/485 (klein) gezeigt. Die Verdrahtung des RS485 Busses entnehmen Sie den nachfolgenden Beispielen.



Achtung:

Achten Sie bei den Beispielen auf die angegebene Hardwareversion, die für das jeweilige Beispiel Voraussetzung ist.



Übergang von RS232 auf RS485

Der Umsetzer tritt an die Stelle des ZK-MasterIV und wird mit einem Sup-D-9-poligen 1:1 Kabel an den PC angeschlossen.

5.7.3. Kommunikation RS 485

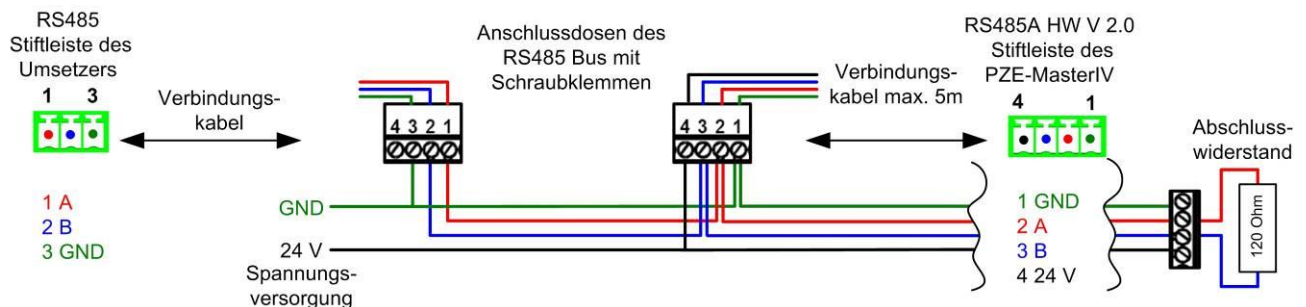
Um über RS485 mit einem Gerät kommunizieren zu können, muss das Gerät für diese Kommunikationsart im Systemmenü-Bios eingestellt sein. Zusätzlich sind Baudrate, Busnummer und Timeout der RS485-Schnittstelle des Terminals und der RS484-Schnittstelle des PCs aufeinander abzustimmen. Als Baudrate sind zulässig 9600, 19200 sowie 38400. Der Timeout muss zwischen 100 und 2000 liegen. Standardmäßig wird der Timeout bei Auswahl der Kommunikationsart RS485 auf 100 gesetzt.

Anschlüsse, Kabelbelegungen und Übergänge von RS 232 auf RS 485 finden Sie im Kapitel „Anschluss“.



Achtung:

Die RS 485 Schnittstelle (4 pol. Stecker) der Hauptkommunikation ist nicht zu verwechseln mit der RS 485 Schnittstelle (8 pol. Stecker) der Zutrittskontrolle.



Anschluss des ZK-MasterIV per RS485 (Stiftleiste)

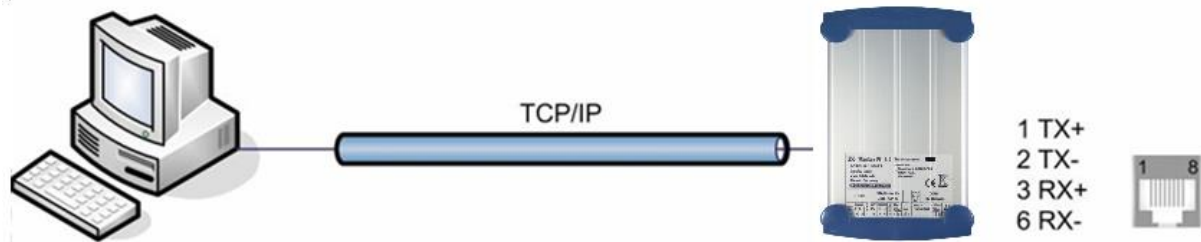


Achtung:

Wird die Spannungsversorgung des ZK-MasterIV und des RS485 Bus über PIN 7/8 (RJ45 Anschluss des Gerätes – siehe Abb.) bzw. über PIN 1/4 (Stiftleiste des Gerätes – siehe Abb.) hergestellt, muss Gleichspannung verwendet werden.

5.7.4. Kommunikation über TCP/IP

Ein Gerät mit TCP/IP-Option kann über die Ethernet Schnittstelle auf der Rückseite des Gerätes mit dem Netzwerk verbunden werden. Soll das Gerät direkt an einen PC per Ethernet angeschlossen werden, muss ein Crossover Kabel zum Einsatz kommen.



Anschluss des ZK-MasterIV per Ethernet



Achtung:

Power over Ethernet (PoE) bezeichnet ein Verfahren, mit dem netzwerkfähige Geräte über das 8-adrige Ethernet-Kabel mit Spannung versorgt werden. Das interne TCP/IP-Modul des Gerätes ist nicht PoE-kompatibel.

5.7.4.1. Einstellung der IP-Adresse

Das Einstellen der IP muss im BIOS-Menü erfolgen.

The image shows a sequence of steps for configuring the IP address. At the top, a BIOS window titled 'Gerätekonfiguration (BIOS)' is shown. The left sidebar has 'LAN MasterIV' selected. The main area is 'Netzwerkkonfiguration' with the following settings:

- IP-Adresse automatisch beziehen:
- Folgende IP-Adresse verwenden: 192 . 168 . 98 . 188 (Port: 8000)
- Subnet: Standard Netmask
- Gateway: 192 . 168 . 98 . 111
- Keepalive: 45 Sekunden

 Below this is the 'Optionen' section with 'Fernzugriff auf die Konfiguration erlauben (z.B. per Telnet)' checked. A red box highlights the IP '192.168.123.221' in the browser address bar, with a red arrow pointing to the 'Folgende IP-Adresse verwenden' field in the BIOS.

Two callout boxes provide instructions:

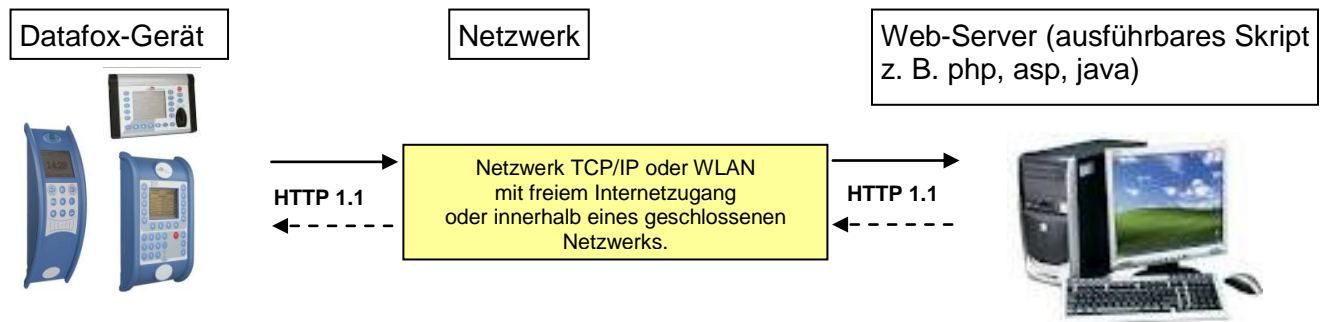
- 'Hier ist es möglich das Gerät auf DHCP zu stellen.' with an arrow pointing to the 'IP-Adresse automatisch beziehen' radio button.
- 'Diese Option ermöglicht den Fernzugriff auf das Web-Interface.' with an arrow pointing to the 'Fernzugriff auf die Konfiguration erlauben' checkbox.

At the bottom, two browser screenshots are shown:

- The left screenshot shows the 'Home' page of the 'LANTRONIX XPort Device Server Configuration Manager Version 1.9.0.1'.
- The right screenshot shows the 'Network Settings' page, where 'Use the following IP configuration' is selected, and the IP address is set to '192.168.123.221'.

5.7.4.2. Versenden von Datensätzen mit HTTP über LAN / WLAN

Bislang war es möglich, die im Gerät erstellten Datensätze mit HTTP über das Mobilfunknetz GPRS an einen Web-Server zu senden. Diese Funktionalität wurde nun auch auf das LAN ausgeweitet.



An jedem Gerät, welches eine TCP/IP Schnittstelle hat, können Sie im Bios-Menü des Gerätes unter Kommunikation HTTP aktivieren. Dazu ist der Eintrag „http“ auf „JA“ abzuändern.

Voraussetzung für das Senden der Daten mit HTTP über LAN, sind die richtigen Einstellungen der Parameter in der **.ini Datei** und die Kommunikation muss auf TCP/IP stehen.

Weitere Informationen zum Bios-Menü des Gerätes erhalten Sie im Kapitel „Aufbau Display im Bios-Menü“.

Mehr zum Thema Verschlüsselung der Daten beim Versenden über HTTP finden Sie in Handbuch DatafoxStudioIV unter dem Kapitel „[Konfiguration > Verschlüsselung der Datenfelder beim Versand per HTTP](#)“.



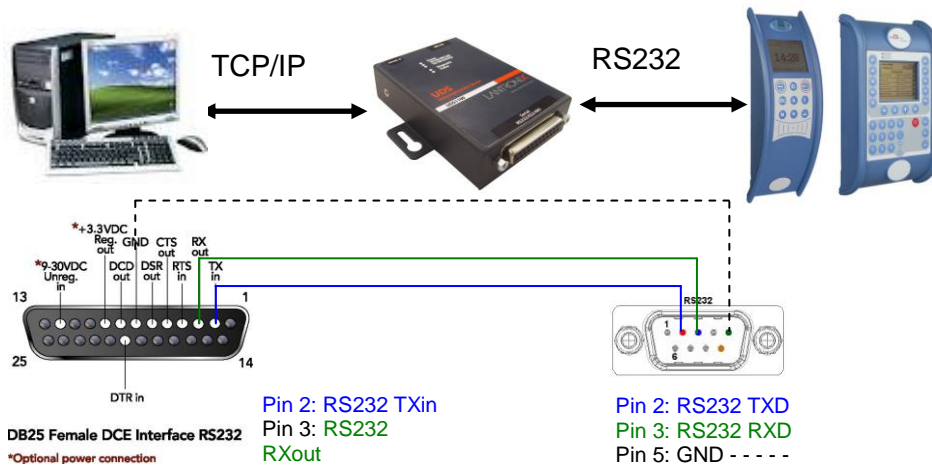
Achtung:

Nicht alle Firewalls lassen eine Übertragung per HTTP zu. Mit der Cisco-Firewall V5.0 treten hin und wieder Probleme auf.

5.7.4.3. Übergang von TCP/IP auf RS232 / RS485 über Comserver

TCP/IP zu RS232

Für den Anschluss eines einzelnen Gerätes mit RS232 an ein TCP/IP Netzwerk muss ein COM-Server eingesetzt werden. Dieser COM-Server (UDS110) dient als Vermittler zwischen den beiden Kommunikationsarten.

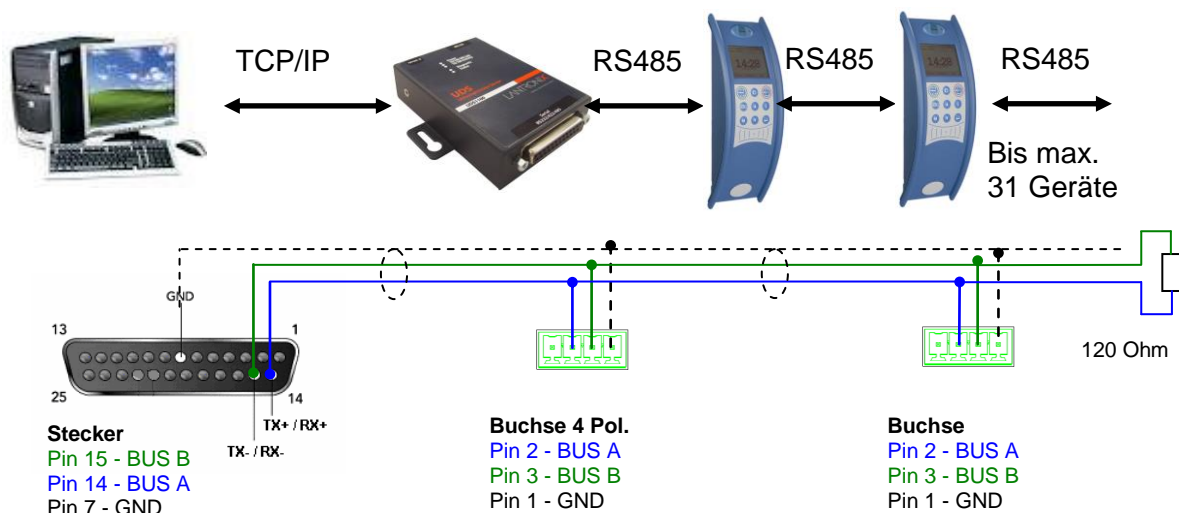


Übergang von TCP/IP auf RS232

TCP/IP zu RS485

Bis zu 31 Geräte können sehr kostengünstig über einen COM-Server mit RS485-Bus angeschlossen werden. Einzelheiten zum Aufbau eines RS485-Netzwerkes finden Sie in der separaten Vernetzungsbeschreibung. Diese können Sie bei uns anfordern oder auf unserer Homepage downloaden. Bitte beachten Sie, dass die Busnummer direkt am Terminal eingestellt werden muss.

Die Struktur des Netzwerkes ist ein Bus. Das Buskabel wird von einem zum nächsten Gerät durchgeschleift. Abzweigungen sind nicht erlaubt. Der Comserver kann am Anfang, am Ende oder irgendwo in der Mitte des Netzwerkes angeschlossen werden. Die Gesamtlänge des Buskabels darf 1000 m nicht überschreiten.



Übergang von TCP/IP auf RS485

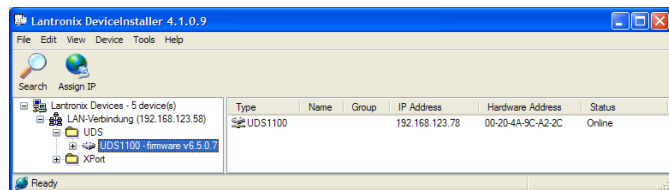
5.7.4.4. Einrichtung des Comserver Lantronix UDS 11

Um die Einrichtung vornehmen zu können, müssen Sie den „Device Installer“ auf der beiliegenden CD installieren und starten.

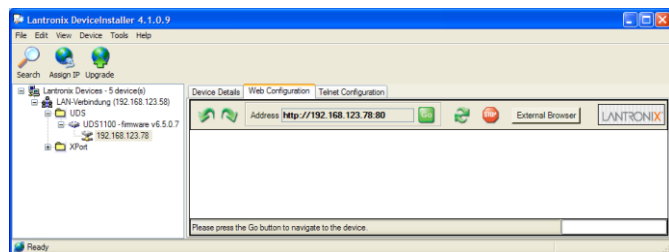
Nach der erfolgreichen Installation binden Sie bitte den Comserver in Ihrem Netzwerk ein. Mit dem beiliegenden Netzteil ist die Spannungsversorgung sicherzustellen und das Netzwerkkabel einzustecken.

Starten Sie nun den „Device Installer“.

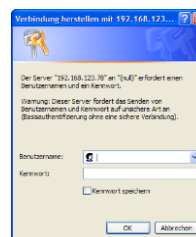
Es werden nun alle „Lantronix Comserver“ angezeigt, die sich im Netzwerk befinden. In diesem Beispiel ein Comserver mit der „IP-Adresse 192.168.123.78“. Sollten Sie mehrere Comserver angezeigt bekommen, orientieren Sie sich an den „Hardware Adressen“ (MAC-Adresse).



Wenn Sie die „IP-Adresse“ blau hinterlegen, kann über eine „Web Configuration“ die Einstellung des Comservers vorgenommen werden. Kopieren Sie dazu die „Adresse“ in Ihren eigenen Browser oder starten Sie direkt mit „Go“, um den vorhandenen Browser zu nutzen.



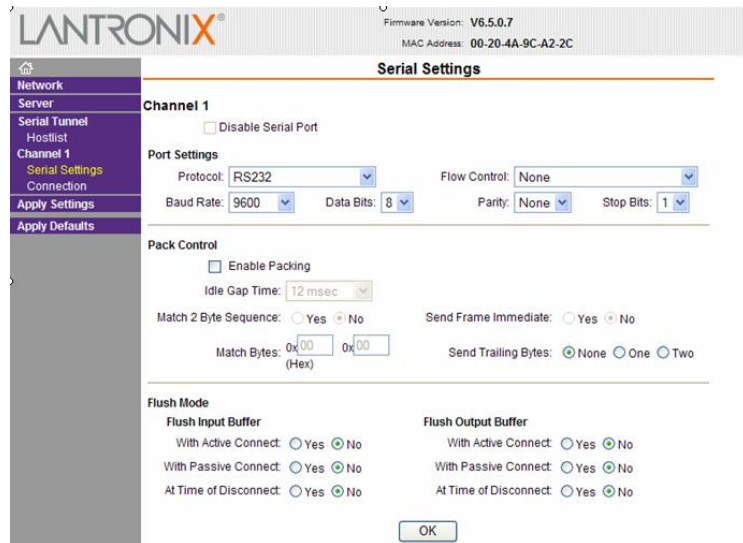
Sie werden nun nach einem Benutzernamen und Kennwort gefragt. Da sich der Comserver im Auslieferungszustand befindet, ist kein Benutzer und Kennwort hinterlegt. Bitte bestätigen Sie ohne eine Eingabe direkt mit „OK“.



RS232

Einstellungen der seriellen Schnittstelle für RS232:

1. Die Baudrate ist auf 38400 einzustellen.



The screenshot shows the LANTRONIX web interface for configuring serial settings. The top bar displays the LANTRONIX logo, Firmware Version: V6.5.0.7, and MAC Address: 00-20-4A-9C-A2-2C. The main content area is titled "Serial Settings" and is divided into several sections:

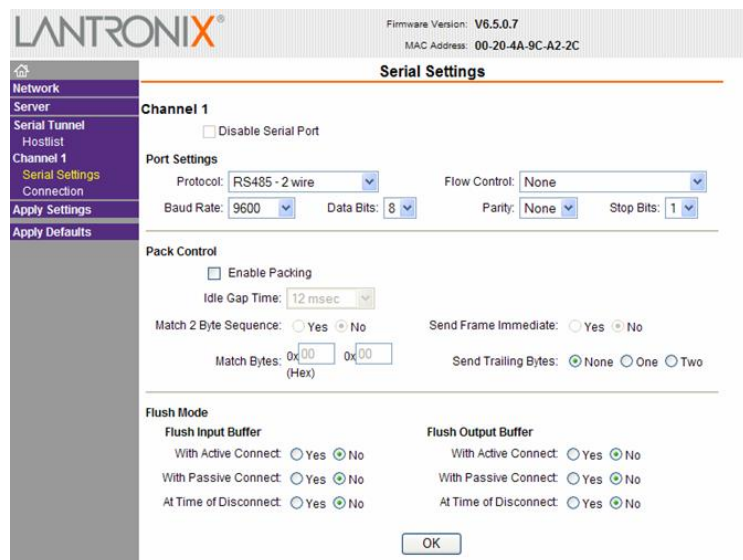
- Channel 1:** Includes a checkbox for "Disable Serial Port".
- Port Settings:**
 - Protocol: RS232
 - Baud Rate: 9600
 - Data Bits: 8
 - Parity: None
 - Stop Bits: 1
 - Flow Control: None
- Pack Control:**
 - Enable Packing:
 - Idle Gap Time: 12 msec
 - Match 2 Byte Sequence: Yes No
 - Match Bytes: 0x00 0x00 (Hex)
 - Send Frame Immediate: Yes No
 - Send Trailing Bytes: None One Two
- Flush Mode:**
 - Flush Input Buffer:**
 - With Active Connect: Yes No
 - With Passive Connect: Yes No
 - At Time of Disconnect: Yes No
 - Flush Output Buffer:**
 - With Active Connect: Yes No
 - With Passive Connect: Yes No
 - At Time of Disconnect: Yes No

An "OK" button is located at the bottom right of the configuration area.

RS485 – 2 wire

Einstellungen der seriellen Schnittstelle für RS485 - 2 wire:

1. Die Baudrate ist im Standard auf 38400 einzustellen.



The screenshot shows the LANTRONIX web interface for configuring serial settings. The top bar displays the LANTRONIX logo, Firmware Version: V6.5.0.7, and MAC Address: 00-20-4A-9C-A2-2C. The main content area is titled "Serial Settings" and is divided into several sections:

- Channel 1:** Includes a checkbox for "Disable Serial Port".
- Port Settings:**
 - Protocol: RS485 - 2 wire
 - Baud Rate: 9600
 - Data Bits: 8
 - Parity: None
 - Stop Bits: 1
 - Flow Control: None
- Pack Control:**
 - Enable Packing:
 - Idle Gap Time: 12 msec
 - Match 2 Byte Sequence: Yes No
 - Match Bytes: 0x00 0x00 (Hex)
 - Send Frame Immediate: Yes No
 - Send Trailing Bytes: None One Two
- Flush Mode:**
 - Flush Input Buffer:**
 - With Active Connect: Yes No
 - With Passive Connect: Yes No
 - At Time of Disconnect: Yes No
 - Flush Output Buffer:**
 - With Active Connect: Yes No
 - With Passive Connect: Yes No
 - At Time of Disconnect: Yes No

An "OK" button is located at the bottom right of the configuration area.

2. In den Einstellungsoptionen „Connection“ ist der „Local Port“ auf 8000 einzustellen.
3. Speichern Sie die geänderten Einstellungen mit „OK“ und danach „**Apply Settings**“ ab, sonst werden diese nicht übernommen.

Starten Sie nun den Comserver neu, und prüfen Sie die Verbindung.

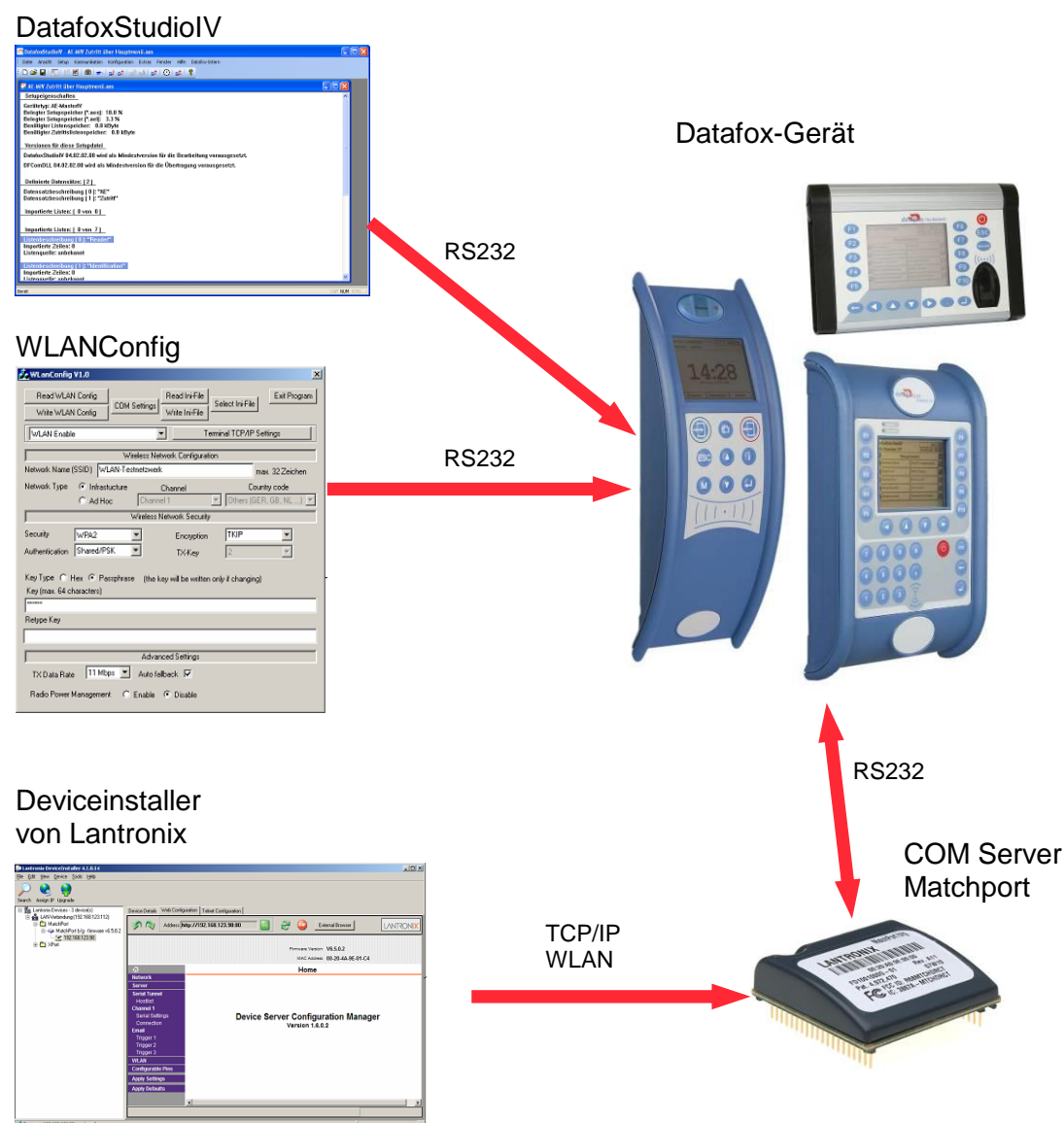
5.7.5. Kommunikation über WLAN

Um über WLAN mit dem Terminal zu kommunizieren, muss dies erst konfiguriert werden. Siehe dazu mehr im nächsten Kapitel.

Bei der Kommunikation über WLAN schließt sich ein Anschluss über LAN aus. Als Schnittstelle unter dem Menüpunkt Kommunikation im Bios des Gerätes, muss TCP/IP eingestellt werden. Mehr über den Aufbau und wie Sie in das Bios-Menü gelangen finden Sie im Kapitel „Bedienung Bios-Menü“.

Konfigurationsmöglichkeiten

Die Konfiguration des Matchportes ist über drei Wege möglich. Der eine ist über TCP/IP mit dem DeviceInstaller™ von Lantronix® und der andere ist per RS232 mit dem Tool WLANConfig und dem DatafoxStudioIV.



Begriffe und Erklärungen

Infrastructure Mode

(Auszug aus Wikipedia, der freien Enzyklopädie)

Der Infrastruktur-Modus ähnelt im Aufbau dem Mobilfunknetz: Eine spezielle Basisstation (Access Point) übernimmt die Koordination aller anderen Netzknoten (Clients). Die Basisstation sendet in einstellbaren Intervallen (üblicherweise zehnmal pro Sekunde) kleine Datenpakete, so genannte „Beacons“ (engl. „Leuchfeuer“), an alle Stationen im Empfangsbereich. Die Beacons enthalten u. a. folgende Informationen:

- Netzwerkname („Service Set Identifier“, **SSID**),
- Liste unterstützter Übertragungsraten,
- Art der Verschlüsselung.

Dieses „Leuchfeuer“ erleichtert den Verbindungsaufbau ganz erheblich, da die Clients lediglich den Netzwerknamen und optional einige Parameter für die Verschlüsselung kennen müssen. Gleichzeitig ermöglicht der ständige Versand der Beacon-Pakete die Überwachung der Empfangsqualität – auch dann, wenn keine Nutzdaten gesendet oder empfangen werden. Beacons werden immer mit der niedrigsten Übertragungsrate (1 MBit/s) gesendet, der erfolgreiche Empfang des „Leuchtfuers“ garantiert also noch keine stabile Verbindung mit dem Netzwerk.

Ad-hoc Mode

(Auszug aus Wikipedia, der freien Enzyklopädie)

Im Ad-hoc-Modus (lat.: "für diesen Augenblick gemacht") ist keine Station besonders ausgezeichnet, sondern alle sind gleichwertig. Ad-hoc-Netze lassen sich schnell und ohne großen Aufwand aufbauen, für die spontane Vernetzung weniger Endgeräte sind allerdings andere Techniken (Bluetooth, Infrarot) eher gebräuchlich.

Die Voraussetzungen für den Ad-hoc-Modus sind dieselben wie für den Infrastruktur-Modus: Alle Stationen benutzen denselben Netzwerknamen („Service Set Identifier“, SSID) und optional dieselben Einstellungen für die Verschlüsselung. Da in dieser Betriebsart keine zentrale Instanz existiert und keine Beacon-Pakete versendet werden, kann ein Client nicht feststellen, ob er sich in Reichweite anderer Stationen mit denselben Einstellungen befindet, wer Teil des Netzes ist und wie es um die Verbindungsqualität bestellt ist. Aus diesen Gründen eignet sich der Ad-hoc-Modus nur für eine sehr geringe Anzahl von Stationen, die sich wegen der begrenzten Reichweite der Sender zudem physisch nahe beieinander befinden müssen. Ist dies nicht der Fall, kann es vorkommen, dass eine Station nicht mit allen anderen Stationen kommunizieren kann, da diese schlicht kein Signal mehr empfangen.

Eine Weiterleitung von Datenpaketen zwischen den Stationen ist nicht vorgesehen und in der Praxis auch nicht ohne weiteres möglich, denn im Ad-hoc-Modus werden keine Informationen ausgetauscht, die den einzelnen Stationen einen Überblick über das Netzwerk geben könnten. Erhebung und Austausch dieser Informationen ist Teil der Aufwertung eines Ad-hoc-Netzwerks zum mobilen Ad-hoc-Netzwerk: Softwarekomponenten auf jeder Station sammeln Daten (z. B. zur „Sichtbarkeit“ anderer Stationen, Verbindungsqualität etc.), tauschen sie untereinander aus und treffen Entscheidungen für die Weiterleitung der Nutzdaten. Die Forschung in diesem Bereich ist noch nicht abgeschlossen und hat neben einer langen Liste von experimentellen Protokollen (OLSR, MIT RoofNet, B.A.T.M.A.N. etc.) und Standardisierungsvorschlägen (Hybrid Wireless Mesh Protocol, 802.11s) auch einige kommerzielle Lösungen (z. B. Adaptive Wireless Path Protocol von Cisco) hervorgebracht.

Frequenzen und Kanäle

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

Sicherheit und Verschlüsselung

(Auszug aus Wikipedia, der freien Enzyklopädie)

Teil des WLAN-Standards IEEE 802.11 ist Wired Equivalent Privacy (**WEP**), ein Sicherheitsstandard, der den RC4-Algorithmus enthält. Die darin enthaltene Verschlüsselung mit einem nur 40 Bit (64 Bit genannt) bzw. 104 Bit (128 Bit genannt), bei einigen Herstellern auch 232 Bit (256 Bit genannt) langen statischen Schlüssel reicht jedoch nicht aus das WLAN ausreichend zu sichern. Durch das Sammeln von Schlüsselpaaren sind Known-Plaintext-Angriffe möglich. Es gibt frei erhältliche Programme, die sogar ohne vollständigen Paketdurchlauf in der Lage sind, einen schnellen Rechner vorausgesetzt, das Passwort zu entschlüsseln. Jeder Nutzer des Netzes kann den gesamten Verkehr zudem mitlesen. Die Kombination von RC4 und CRC wird als kryptografisch unsicher betrachtet.

Aus diesen Gründen sind technische Ergänzungen entwickelt worden, etwa WEPplus, Wi-Fi Protected Access (**WPA**) als Vorgriff und Teilmenge zu 802.11i, Fast Packet Keying, Extensible Authentication Protocol (EAP), Kerberos oder High Security Solution, die alle mehr oder weniger gut das Sicherheitsproblem von WLAN verkleinern.

Der Nachfolger des WEP ist der neue Sicherheitsstandard 802.11i. Er bietet eine erhöhte Sicherheit durch die Verwendung von **TKIP** (Temporal Key Integrity Protocol) bei WPA bzw. Advanced Encryption Standard (AES) bei **WPA2** und gilt zur Zeit als nicht zu entschlüsseln, solange keine trivialen Passwörter verwendet werden, die über eine Wörterbuch-Attacke geknackt werden können. Als Empfehlung kann gelten mit einem Passwortgenerator Passwörter zu erzeugen, die Buchstaben in Groß- und Kleinschreibung, Zahlen und Sonderzeichen enthalten und nicht kürzer als 32 Zeichen sind.

CCMP oder auch Counter-Mode/CBC-Mac Protocol ist gemäß IEEE 802.11i ein Kryptographie-Algorithmus. CCMP nennt sich vollständig Counter Mode with Cipher Block Chaining Message Authentication Code Protocol. CCMP basiert auf dem Advanced Encryption Standard (AES). Es wird ein 128-bit starker Schlüssel mit einem 48-bit starken Initialisator für Antwort-Abfragung verwendet.

Authentication

(Auszug aus Wikipedia, der freien Enzyklopädie)

Extensible Authentication Protocol ist ein Protokoll zur Authentifizierung von Clients. Es kann zur Nutzerverwaltung auf RADIUS-Server zurückgreifen. EAP wird hauptsächlich innerhalb von WPA für größere WLAN-Installationen eingesetzt.

Mit Pre-Shared Key ("vorher vereinbarter Schlüssel") oder kurz **PSK** bezeichnet man solche Verschlüsselungsverfahren, bei denen die Schlüssel vor der Kommunikation beiden Teilnehmern bekannt sein müssen, also symmetrische Verfahren. PSK-Verschlüsselung hat den Vorteil, dass sie zwischen zwei bekannten Teilnehmern wesentlich einfacher zu realisieren ist, als asymmetrische Verschlüsselung. Der große Nachteil des Verfahrens besteht darin, dass beide Teilnehmer den Schlüssel vor der eigentlichen Kommunikation im Geheimen tauschen müssen. Daraus folgt, dass das PSK-Verfahren für viele Anwendungen im Internet (wie z. B. Online-Einkauf) ungeeignet ist, da der vorherige Schlüsseltausch in diesem Fall nicht möglich bzw. viel zu aufwendig ist. In einem solchen Fall verwendet man besser das Public-Key-Verfahren.

Kennwörter

(Auszug aus Wikipedia, der freien Enzyklopädie)

Moderne Verschlüsselungsverfahren sind technisch so weit fortgeschritten, dass sie in der Praxis, außer durch das Austesten aller möglichen Schlüssel - der sogenannten Brute-Force-Methode, meist nur durch einen Wörterbuchangriff geknackt werden können. Die Schwachstelle ist bei beiden Angriffen das vom Benutzer gewählte Kennwort (**Key**). Damit ein Kennwort nicht unsicherer ist als die eigentliche Verschlüsselung (112 bis 128-Bit-Schlüssel bei gängigen Verfahren), ist für dieses theoretisch eine Folge von etwa 20 zufälligen Zeichen erforderlich. Falls das Kennwort nicht aus zufälligen Zeichen besteht, sind sogar deutlich längere Zeichenfolgen nötig, um die gleiche Sicherheit zu erreichen.

Da die Länge der Kennwörter, die zur Verschlüsselung verwendet werden können, softwareseitig oft begrenzt ist (zum Beispiel bringen Kennwörter mit mehr als 32 Zeichen bei AES keinerlei Sicherheitsgewinn), sollte man immer Zeichenkombinationen wählen, die aus seltenen Wörtern und Wortstellungen, Phantasiewörtern oder fremdsprachigen Wörtern, Anfangsbuchstaben eines Satzes, Zahlen und/oder Sonderzeichen oder noch besser Kombinationen davon bestehen. Deren Bestandteile sollten für einen gut über die Person und ihre Interessen informierten Angreifer nicht vorhersehbar sein. Eine Alternative ist es, einen Kennwortgenerator zu benutzen und sich das Kennwort entweder gut einzuprägen oder an einem geheimen Ort zu notieren.

Ein recht sicheres Kennwort könnte sein: 0aJ/4%(hGs\$df"Y! (16 Zeichen). Die Problematik solcher Zufallszeichenfolgen ist jedoch, dass sie schwer zu merken sind und deshalb irgendwo notiert werden. Eine leichter zu merkende Alternative ist ein einstudierter, zeichenweise veränderter Satz wie „dIE bANANNE*3 durch 1/4 nIKOTIN.“ (32 Zeichen), wichtig ist hier das Einstreuen von genügend Zufallszeichen. Gut geeignet ist die Verwendung der Anfangsbuchstaben eines Satzes („Hd7B%sd7Z“ gebildet aus den fett hervorgehobenen Zeichen von „Hinter den 7 Bergen % sind die 7 Zwerge“, mit eingestreutem Sonderzeichen).

Die Verwendung von Sonderzeichen kann zwar einen Sicherheitsgewinn bringen, da ein Kennwort dadurch komplexer wird. Dennoch ist davon abzuraten, wenn mit der Möglichkeit zu rechnen ist, dass das Kennwort auch im Ausland verwendet werden muss, weil nicht auf allen Tastaturen die gleichen Sonderzeichen vorhanden sind.

Zurücksetzen der WLAN-Einstellungen

Am Terminal kann unter **factory default WLAN** des Menüpunktes Kommunikation des BIOS-Dialogs ein Zurücksetzen auf fest definierte Standwerte erfolgen. Beim Ausführen werden folgende Einstellungen vorgenommen.

WLAN: enabled
 Topology: Infrastructure
 Network name (SSID): WLAN-DATAFOX
 Security: none

Damit Sie mit dem Terminal wieder arbeiten können, müssen Sie die Einstellungen Ihres WLAN-Routers den Standardwerten anpassen. Ist das der Fall, kann mit dem Deviceinstaller von Lantronix das Modul wieder konfiguriert werden.

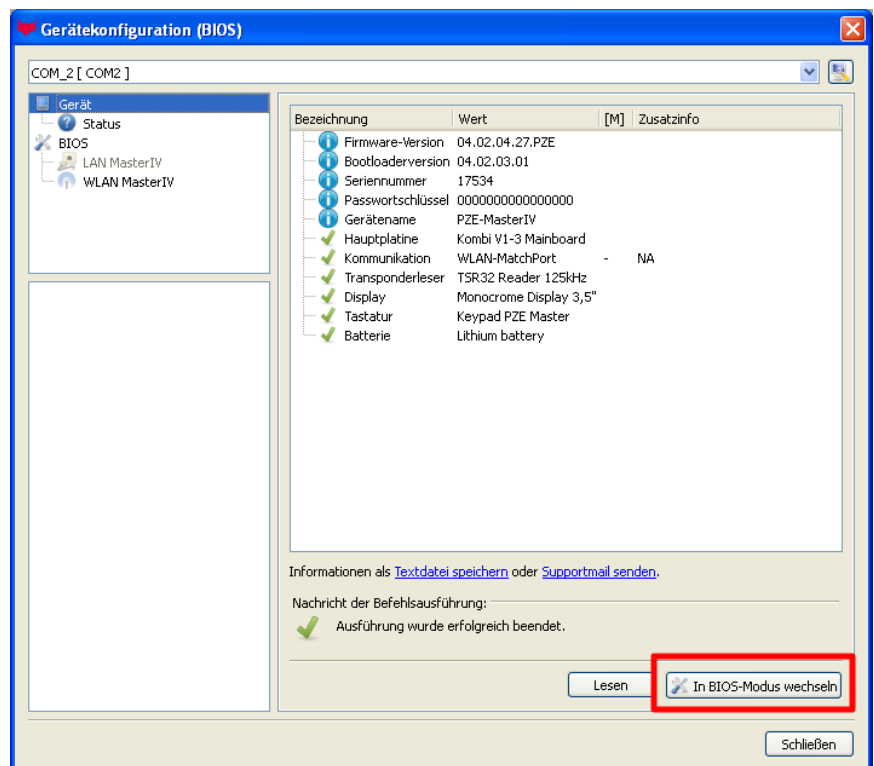
Ein anderer Weg wäre das Programm WLANConfig von Datafox zu verwenden, welches per RS232 auf das Gerät zugreift und von dort her den Matchport konfiguriert. Per RS232 ist immer ein Zugriff auf den Matchport möglich, allerdings muss die Hauptkommunikation dann auf RS232 stehen.

WLAN Einstellung über DatafoxStudioIV

Stellen Sie eine Verbindung zwischen DatafoxStudioIV und dem Gerät über RS232 her. Aktivieren Sie den Bios-Modus des Gerätes. Nach dem Aktivieren sehen Sie diese Masken und können die entsprechenden Einstellungen vornehmen.

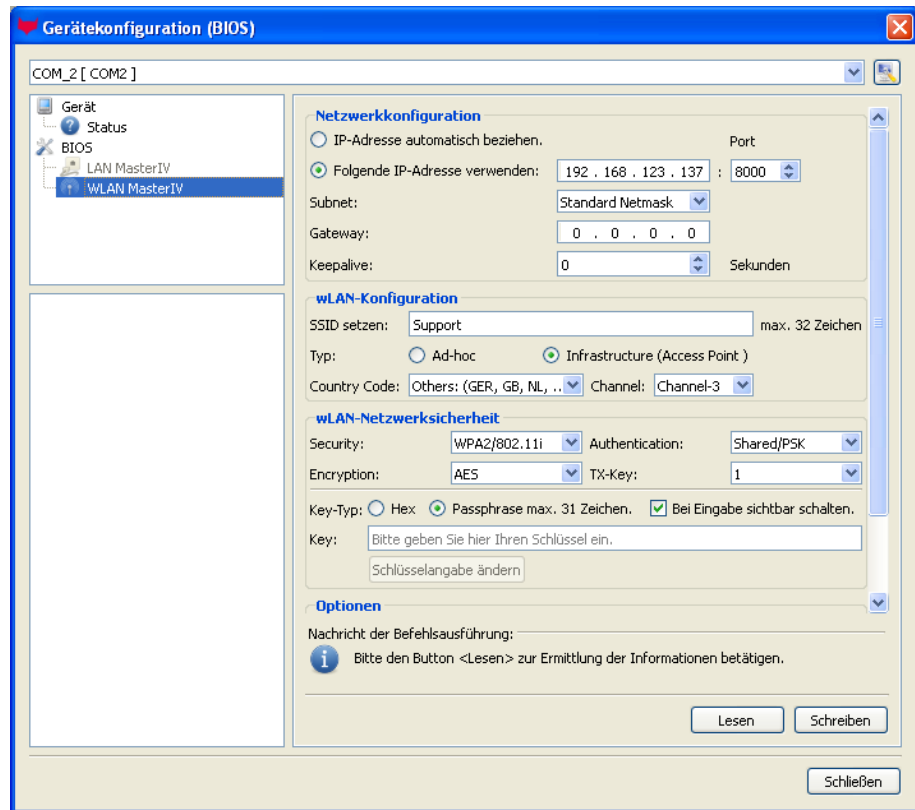
Klicken Sie auf „In dem Bios-Modus wechseln“.

Voraussetzung für das Umschalten in den Bios-Modus ist ein erreichbares Gerät. Erst dann werden die Einstellseiten frei geschaltet.



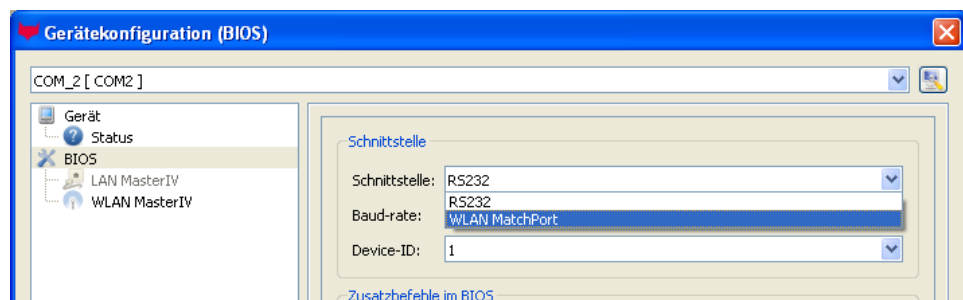
WLAN Parameter für die Verbindung zum Access Point einstellen

Hier können Sie alle notwendigen Einstellungen, welche für TCP/IP und WLAN notwendig sind, vornehmen.

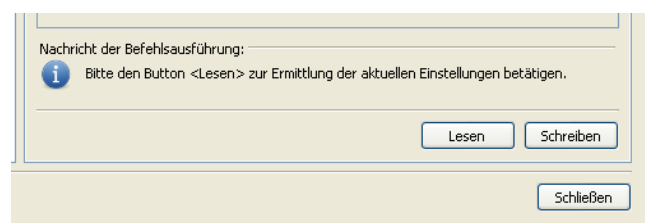


Hauptkommunikation auf WLAN umstellen!

Stellen Sie die Hauptkommunikation auf WLAN um.

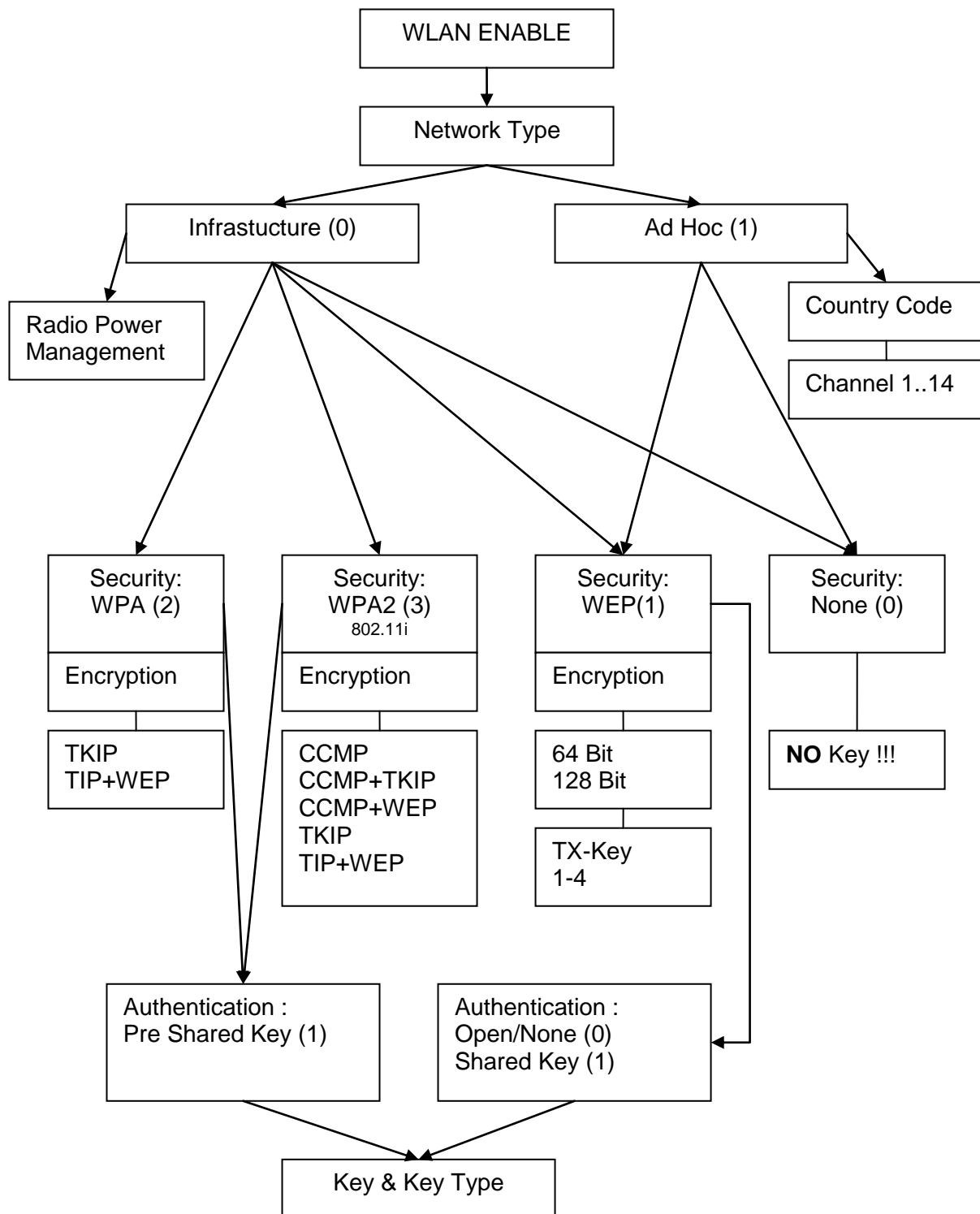


Klicken Sie anschließend auf „Schreiben“.



Abhängigkeiten WLAN

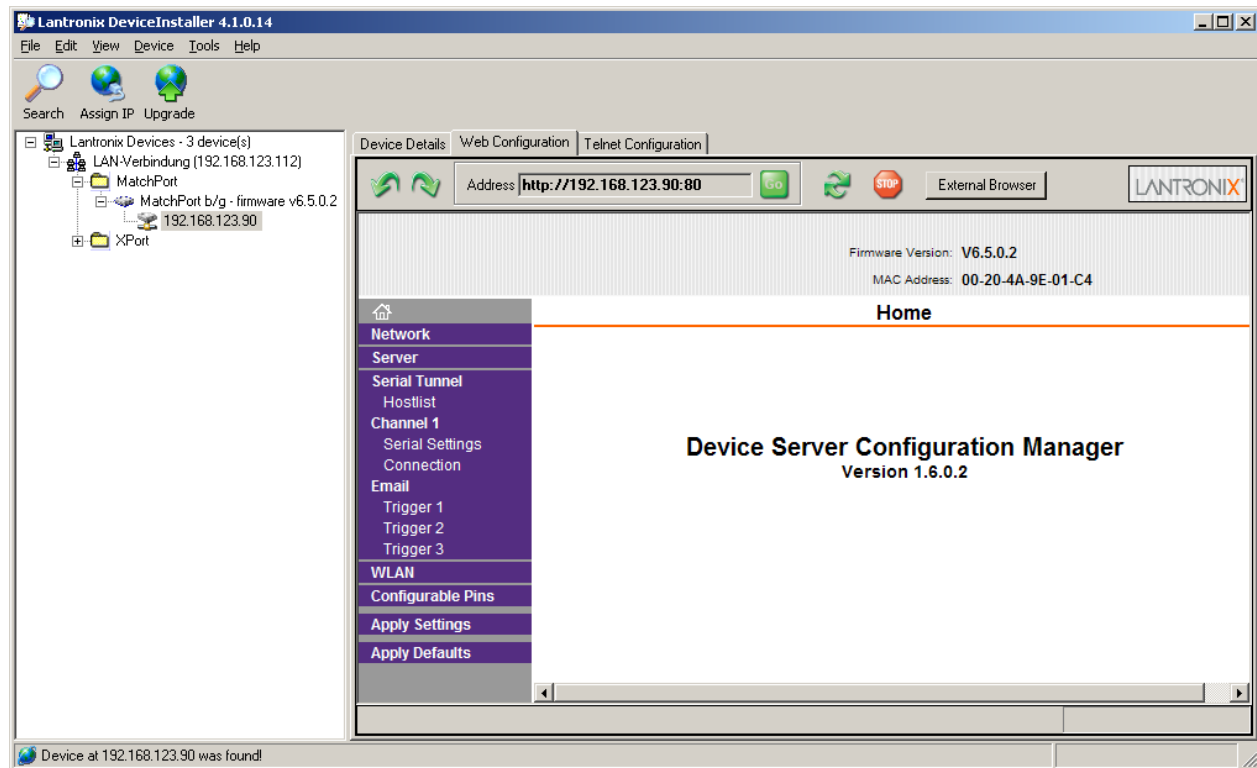
Aufgrund verschiedener Parametriermöglichkeiten ergeben sich gewisse Abhängigkeiten einzelner Parameter.



Der Deviceinstaller von Lantronix

Der DeviceInstaller™ von Lantronix® befindet sich auf der beiliegenden Datafox Produkt DVD unter **DVD:\Datafox-Optionen (eingebaute Module)\LAN, Matchport**.

Mit diesem Tool können bei Datafoxgeräten die Comserver Xport und Matchport konfiguriert werden. Der Deviceinstaller greift über TCP/IP auf den Comserver zu und die Datafox-Terminals greifen per RS232 auf den Comserver zu. Sollte ein Comserver nicht erreichbar sein, weil er so verstellt ist, dass der Deviceinstaller nicht darauf zugreifen kann, kann nur noch über das BIOS-Menü des Terminals der Comserver auf Standardwerte zurückgesetzt werden.



WLANConfig von Datafox

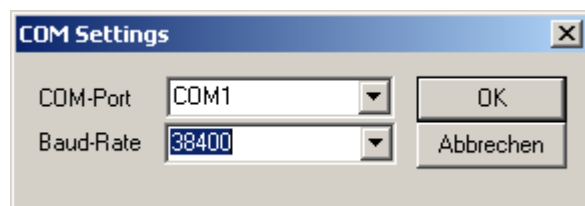
Allgemeines

Das Programm WLANConfig kann die TCP/IP und die WLAN Einstellungen des Matchportes über RS232 setzen. Die Einstellungen können auch in einer Datei gespeichert werden und die Daten dieser Datei in das Gerät übertragen werden. Die Abhängigkeiten von einzelnen Parametern untereinander werden von dem Programm selbst erlaubt oder verriegelt.

Vier Dialoge werden zum Arbeiten mit dem Programm zur Verfügung gestellt.

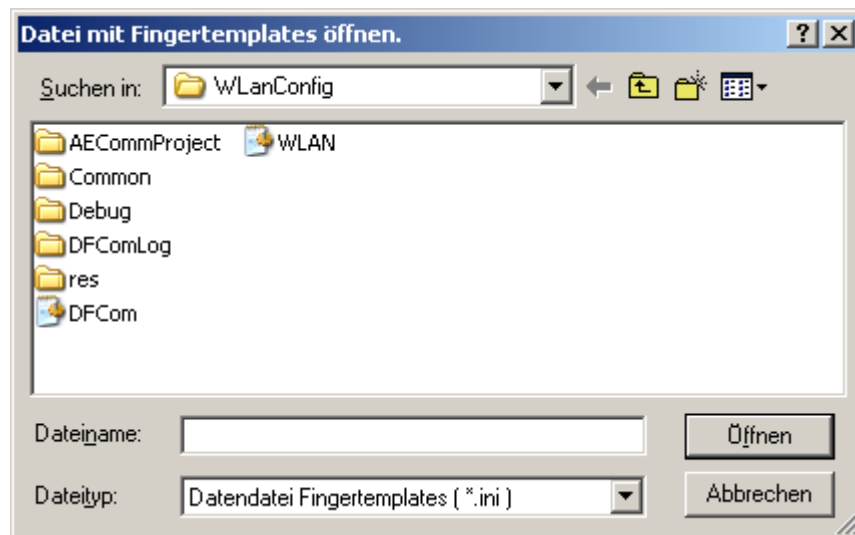
- WLAN-Einstellungen (Hauptdialog)
- Auswahl der Seriellen Schnittstelle (COM-Settings)
- Auswahl der Konfigurationsdatei (Select INI-File)
- TCP/IP-Einstellungen (Terminal TCP/IP Settings)

Auswählen der Seriellen Schnittstelle



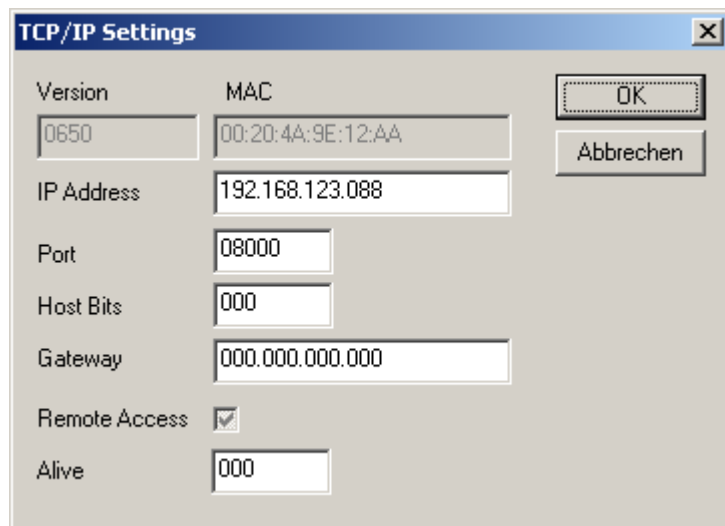
Mit diesem Dialog wird die Schnittstelle am PC ausgewählt an die das Master IV Terminal angeschlossen ist. Die Baudrate ist meistens 38400Baud und muss mit der vom Terminal übereinstimmen. Der Dialog wird durch Drücken der Taste COM Settings ausgeführt.

Auswahl der Konfigurationsdatei



Über den Select INI-File Button wird der Dialog gestartet und ermöglicht das Auswählen einer Datei in der die Daten abgelegt sind bzw. der Dialog kann auch eine neue Datei erstellen. In der Ini-Datei sind alle Einstellungen für TCP/IP und WLAN abgelegt.

TCP/IP Einstellungen



Version	MAC	OK
0650	00:20:4A:9E:12:AA	Abbrechen
IP Address	192.168.123.088	
Port	08000	
Host Bits	000	
Gateway	000.000.000.000	
Remote Access	<input checked="" type="checkbox"/>	
Alive	000	

Der Dialog wird über den Button Terminal TCP/IP Settings aufgerufen. Es wird die aktuelle Firmwareversion des Matchportes angezeigt, sowie die MAC-Adresse. Die anderen Parameter sind editierbar und gleich dem BIOS-Dialog des Terminals und auch des Datafox Studios.

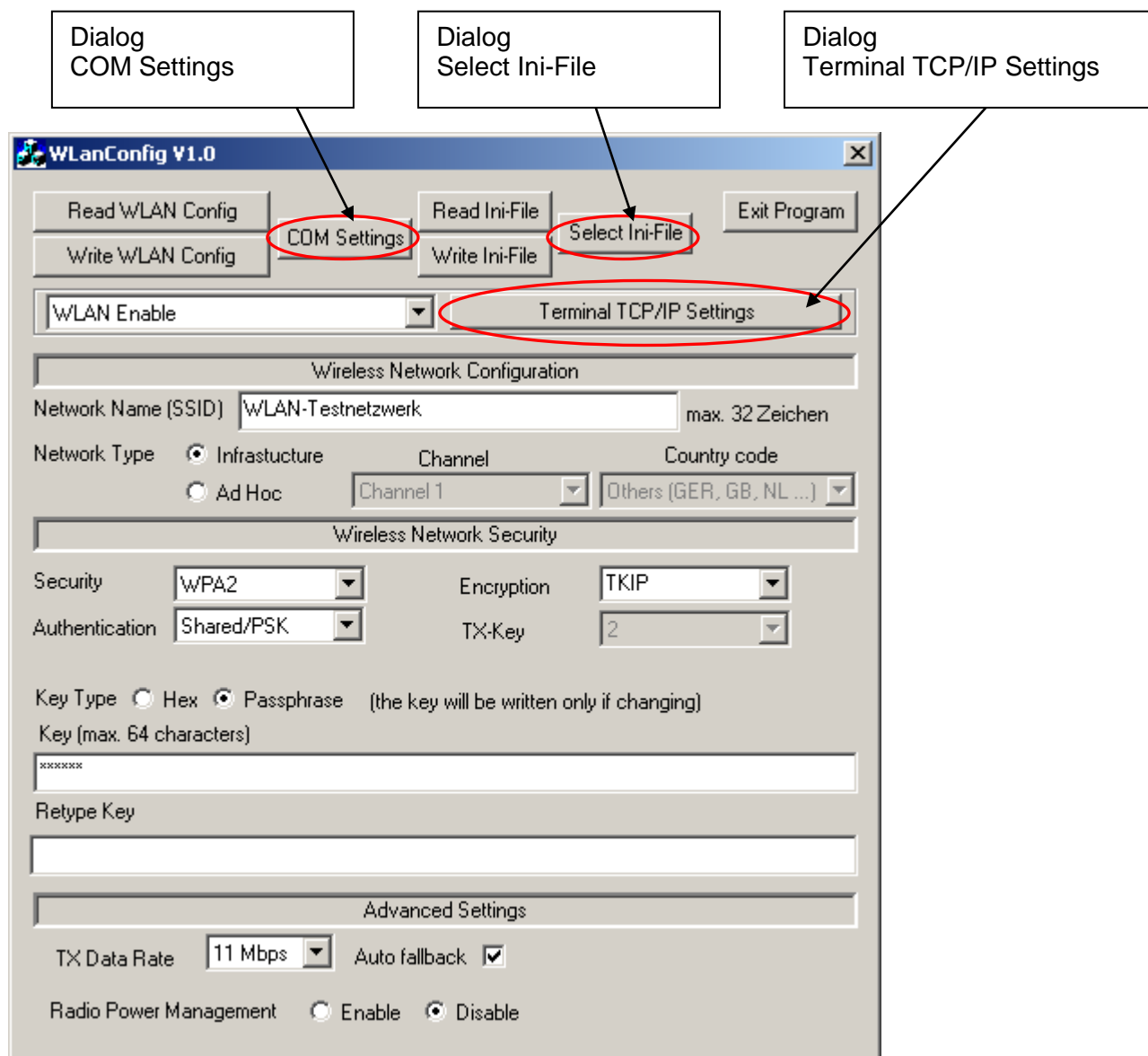
WLAN Einstellungen

Die WLAN Einstellungen ermöglichen das Editieren von Werten, die aus dem Terminal gelesen wurden, aus einer Ini-Datei geladen wurden oder von Hand eingetragen worden sind. Wichtig ist, dass der Key aus dem Terminal nicht gelesen werden kann. Er wird auch nicht zurückgeschrieben, wenn er nicht eingegeben worden ist. Ist in der Ini-Datei der Key vorhanden, wird nach dem Laden der Daten bei beiden Key-Editfeldern eine Gruppe von * Zeichen angezeigt und er wird auch mit in das Gerät übertragen. Um WLAN benutzen zu können, muss WLAN Enable eingestellt werden. Dieser Parameter kann vom Deviceinstaller von Lantronix ebenfalls eingestellt werden. Wenn man über WLANConfig mehrere Geräte konfigurieren will, muss man beachten, dass die IP-Adresse in den Geräten mit gesetzt wird.



Achtung:

Nach dem Übertragen der Parameter muss das Gerät von RS232 auf TCP/IP umgestellt werden, damit der Matchport aktiviert wird. Erst dann ist er im Netzwerk verfügbar.



Mit Read WLAN Config werden die Daten aus dem Gerät in das Programm geladen.

Mit Write WLAN Config werden die Daten vom Programm in das Gerät geladen.

Mit Read Ini-File werden die Daten aus der gewählten Datei in das Programm geladen.

Mit Write Ini-File werden die Daten vom Programm in die Datei geschrieben.

5.7.6. Kommunikation über USB

USB an PC



Das MasterIV-Gerät wird über ein Standard USB Kabel A auf mini USB-B an einen PC angeschlossen.



Achtung:

Für die Kommunikation mit dem ZK-MasterIV 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.

Um die Kommunikation über USB nutzen zu können, müssen Sie die notwendigen USB-Gerätetreiber und die Treiber für den USB-Seriell-Converter installieren.

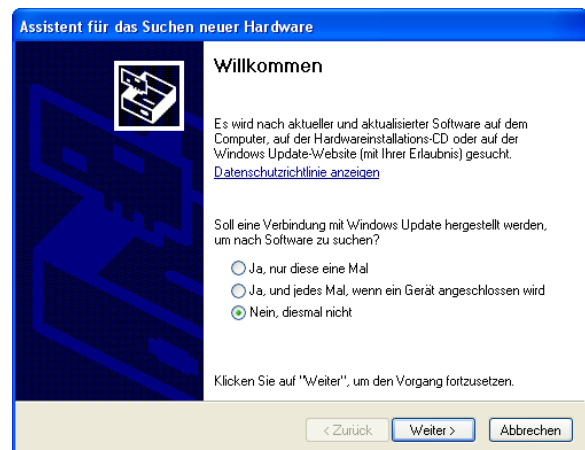


Achtung:

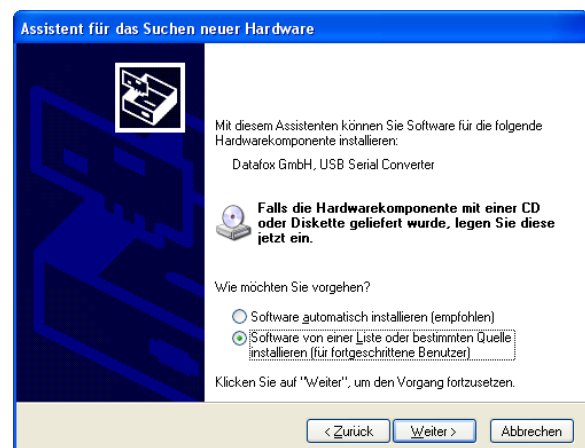
Es sind nur die zum Gerät mitgelieferten Treiber zu verwenden.

Treiberinstallation USB

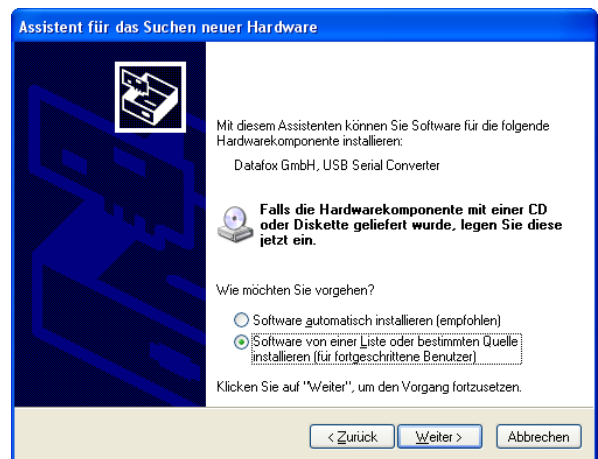
Nachdem Sie den MasterIV an den PC angeschlossen haben, wird das Terminal als neues USB-Device erkannt und es beginnt die Installation der mitgelieferten USB-Treiber.



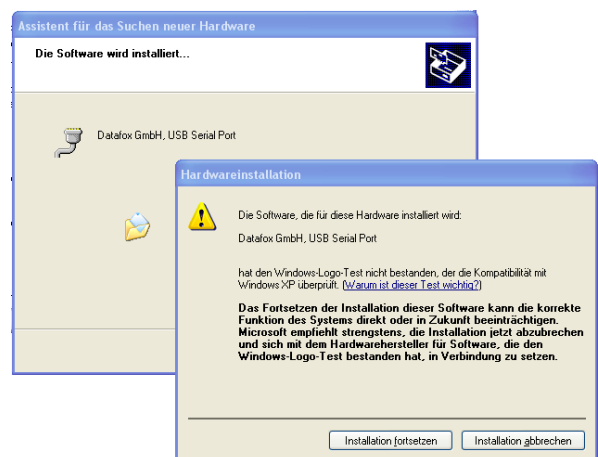
Nachdem Sie den MasterIV an den PC angeschlossen haben, wird das Terminal als neues USB-Device erkannt und es beginnt die Installation der mitgelieferten USB-Treiber.



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

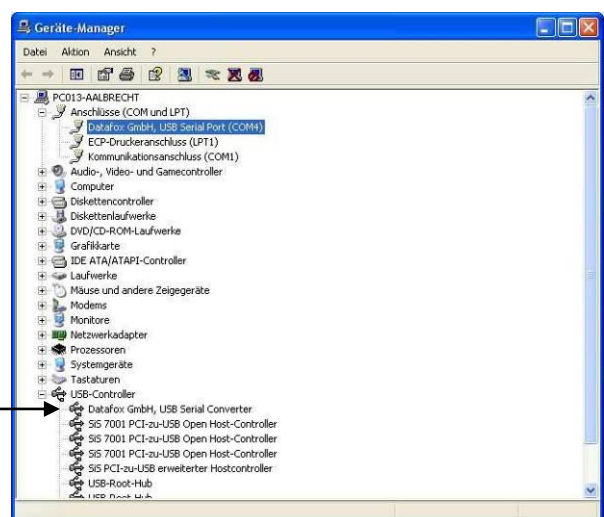


Installation der Treiber für den virtuellen COM Port. Auch bei diesem Installationsschritt erhalten Sie die Meldung, dass der Treiber den Microsoft Logo-Test nicht bestanden hat. Hier müssen Sie ebenfalls auf „Installation fortsetzen“ klicken, um den Treiber nutzen zu können.



Zusätzlich ist im Geräte-Manager der Eintrag für den Datafox USB Seriell Port hinzugekommen. Über diesen COM-Port können Sie mit dem DatafoxStudioIV oder Ihrer eigenen Anwendung über die DFComDLL.dll eine Verbindung zum MasterIV Gerät aufbauen.

Den erfolgreichen Abschluss der Installation der USB Treiber können Sie im Geräte-Manager prüfen. Es müssen folgende Einträge ohne gelbes Ausrufungszeichen angezeigt werden.



USB-Stick als Datenträger

Zusätzlich zur Hauptkommunikation USB gibt es die Möglichkeit, einen USB Stick als Datenträger zu verwenden. Sie können so Datensätze aus einem ZK-MasterIV auslesen und mit einem PC weiterverarbeiten bzw. Listen für Stammdaten und Zutrittskontrolle in das Terminal laden.

Die ersten Schritte, um den Datentransfer zwischen Terminal und USB-Stick zu gewährleisten, ist das Anlegen der Verzeichnisstruktur auf dem USB-Stick.

Dazu nutzen Sie bitte das DatafoxStudioIV.

Eine vollständige Beschreibung der notwendigen Einrichtung des USB-Stick finden Sie im Handbuch "DatafoxStudioIV".

Passwort und Kommunikationssicherheit

Wie ein Passwort für die Kommunikation zum USB-Stick hinterlegt wird, finden Sie im Handbuch „DatafoxStudioIV“.

Es ist auch möglich Daten für einzelne Terminals separat auf dem Stick zu hinterlegen.

Mehr dazu im Handbuch „DatafoxStudioIV“.

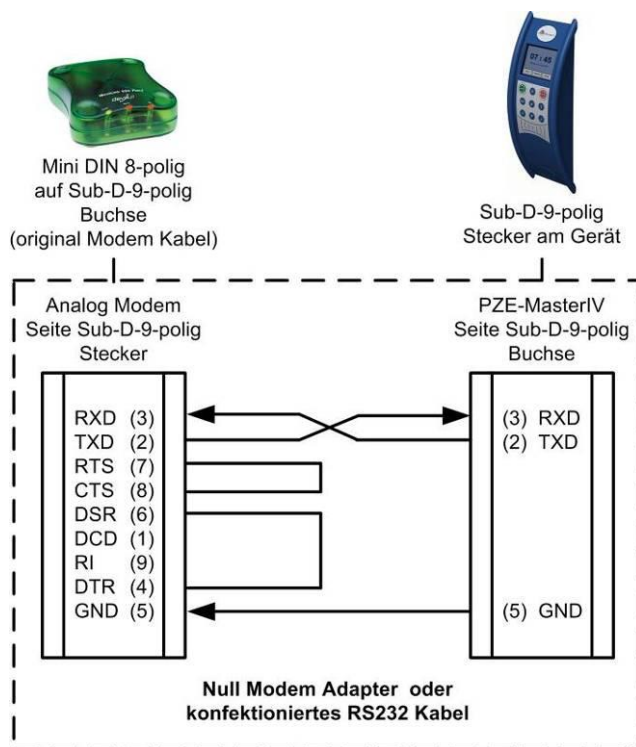
5.7.7. Kommunikation über Modem

Das analoge Modem wird an die COM-Schnittstelle des Gerätes angeschlossen. Für den Anschluss ist ein Null-Modem-Adapter oder ein entsprechend der Abbildung konfektioniertes Kabel zu verwenden. Achten Sie darauf, dass auf der Seite des Gerätes keine Anschlüsse gebrückt sind.



Hinweis:

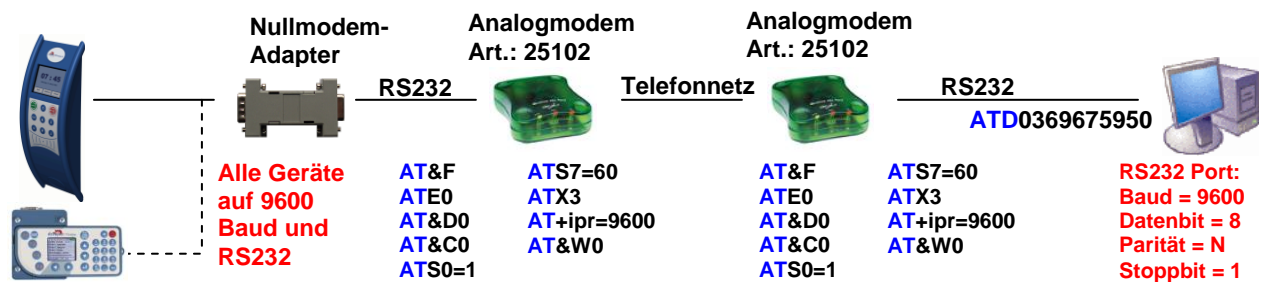
Achten Sie darauf, dass die Hauptkommunikation auf RS232 steht und die Baudrate des Modems auf die Baudrate des Gerätes eingestellt ist. Das Modem muss vor dem Einsatz konfiguriert werden.



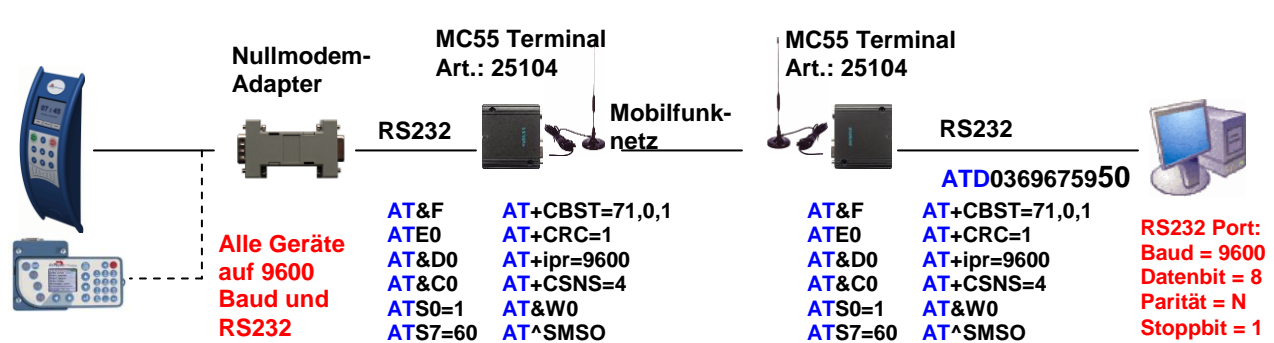
Achten Sie darauf, dass auf der Seite des MasterIV-Gerätes keine Anschlüsse gebrückt sind. Zwischen einem Null-Modem-Adapter und dem Terminal können Sie als Verlängerung ein Sub-D-9-poliges 1:1 Kabel verwenden.

Für die Kommunikation über ein analoges Modem muss im Systemmenü-Bios des Gerätes die Kommunikationsart „RS232“ eingestellt sein. Die Baudrate des Terminals muss mit der Baudrate des angeschlossenen Modems übereinstimmen. Der Timeout ist in Abhängigkeit von der Leitungsqualität des Telefonnetzes (Welchen Störquellen ist die Leitung ausgesetzt?) einzustellen. Je schlechter die Leitungsqualität desto höher sollte der Timeout eingestellt werden. Das Modem, an welchem das Terminal angeschlossen werden soll, muss über die COM-Schnittstelle eines PC's konfiguriert werden. Die im Folgenden aufgeführten Schritte beziehen sich auf das getestete und empfohlene „Devol-MicroLink 56 k Fun II“ Modem.

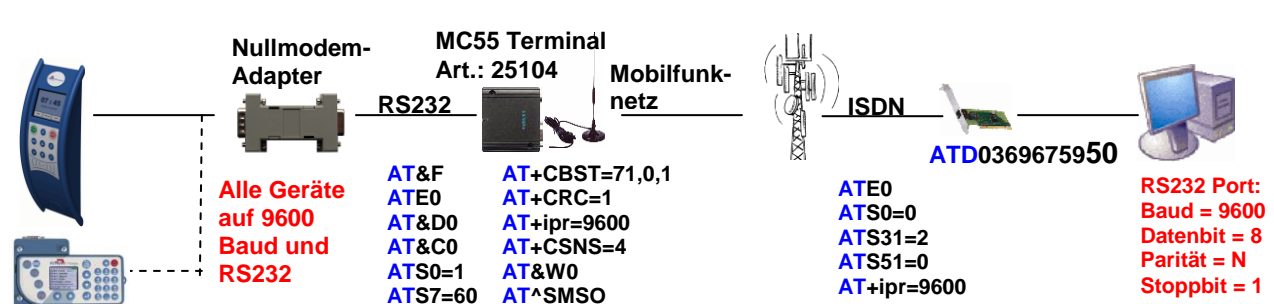
Analogmodem zu Analogmodem



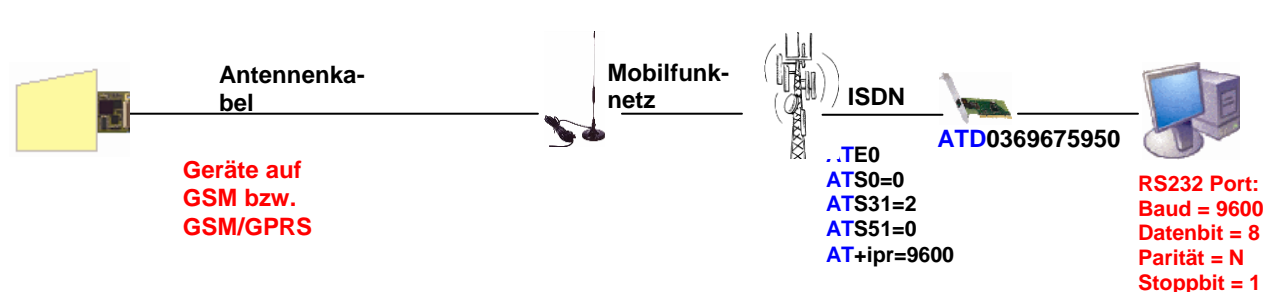
Mobilfunkmodem zu Mobilfunkmodem



ISDN (Festnetz) zu Mobilfunkmodem



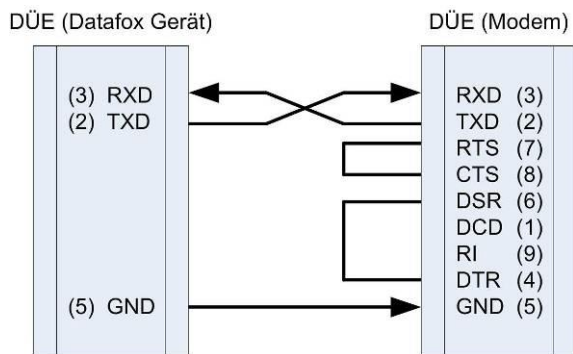
ISDN (Festnetz) zu MC55 (im Gerät intern verbaut)



Hinweis:

Die oben aufgeführten Konfigurationen sind keine Garantie für einen Verbindungsaufbau. Sie beruhen lediglich auf Erfahrungswerten und müssen bei verschiedenen Telefonanlagen u. U. angepasst werden. Konfigurationen, die hier nicht aufgeführt wurden, funktionieren in der Regel auch nicht.

Verbindungsleitung Datafox-Gerät und Modem



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

Abkürzung	Beschreibung
DCD	Wird aktiviert, wenn das angeschlossene Modem mit einem anderen Modem eine Verbindung aufgenommen hat. Somit weiß der PC, dass eine Verbindung besteht und Daten gesendet werden können.
DTR	Hiermit signalisiert ein Rechner, z.B. bei einer Direktverbindung, seine Betriebsbereitschaft.
DSR	Als Antwort auf DTR. (bei gekreuzten Leitungen)
RTS	Wird aktiv, wenn ein Endgerät bereit ist Daten zu senden.
CTS	Wird aktiv, wenn ein Endgerät bereit ist Daten zu empfangen.
RI	Wird von einem angeschlossenen Modem bei einem eingehenden Ruf erzeugt.

Ausgänge:

Low-Pegel = + 12 V High-Pegel = - 12 V Ausgangsstrom: bis zu 10 mA

Eingänge:

Low-Pegel wird erkannt bis ca. + 1 V High-Pegel wird erkannt ab ca. + 1 V Eingangswiderstand = 10 kOhm

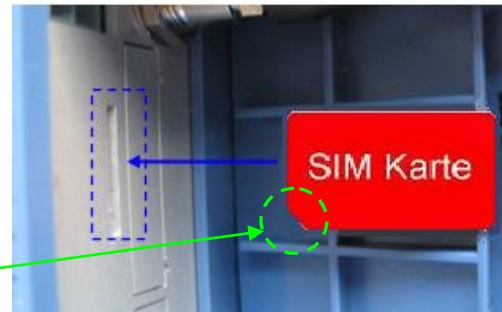
Verbindungsaufbau über das DatafoxStudioIV

Nutzen Sie hierzu das Handbuch DatafoxStudioIV. Im Kapitel „Gerätewartung über Modem“ finden Sie alle notwendigen Informationen.

5.7.8. Kommunikation über Mobilfunk (GSM bzw. GPRS/GSM)

Der ZK-MasterIV 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 ZK-MasterIVs eingesteckt.

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



Achten Sie auf die abge-schrägte Kante.

Stecken Sie nun die SIM-Karte ein.

Verwenden Sie zum Einschleiben ein Hilfsmittel, wie z.B. ein Stift oder Schraubendreher.

Die SIM-Karte muss merklich einrasten.



Achtung:

Zum Einschleiben 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.

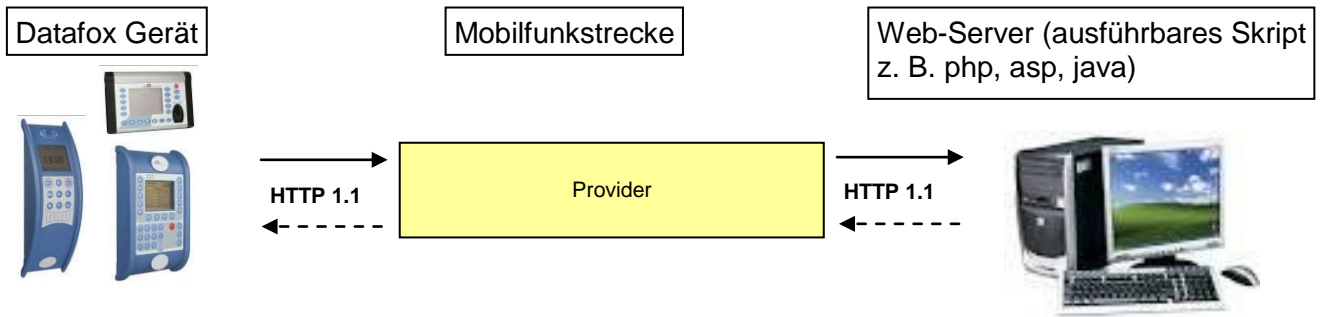
Informationen zu M2M:

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

5.7.8.1. Notwendige Einstellungen für die Kommunikation über das Mobilfunknetz

Um über Mobilfunk eine Kommunikation zu ermöglichen, muss die Hauptkommunikation im Bios des Gerätes auf GPRS umgestellt werden. Wie Sie in das Bios-Menü gelangen, finden Sie im Kapitel [„Biosmenü“](#).

Veranschaulichung zur Verbindung über das Mobilfunknetz.



Weiterhin müssen Angaben wie SIM-Karten Pin, Provider und Einwahlspezifikationen angegeben werden. Diese Angaben werden in einer **GPRS.ini-Datei** gespeichert und in das Gerät geschrieben. Mehr dazu finden Sie im Handbuch DatafoxStudioIV im Kapitel [„Konfiguration Systemvariablen HTTP / GPRS“](#).

Verschlüsselung der Datenfelder beim Versand per HTTP (GPRS)

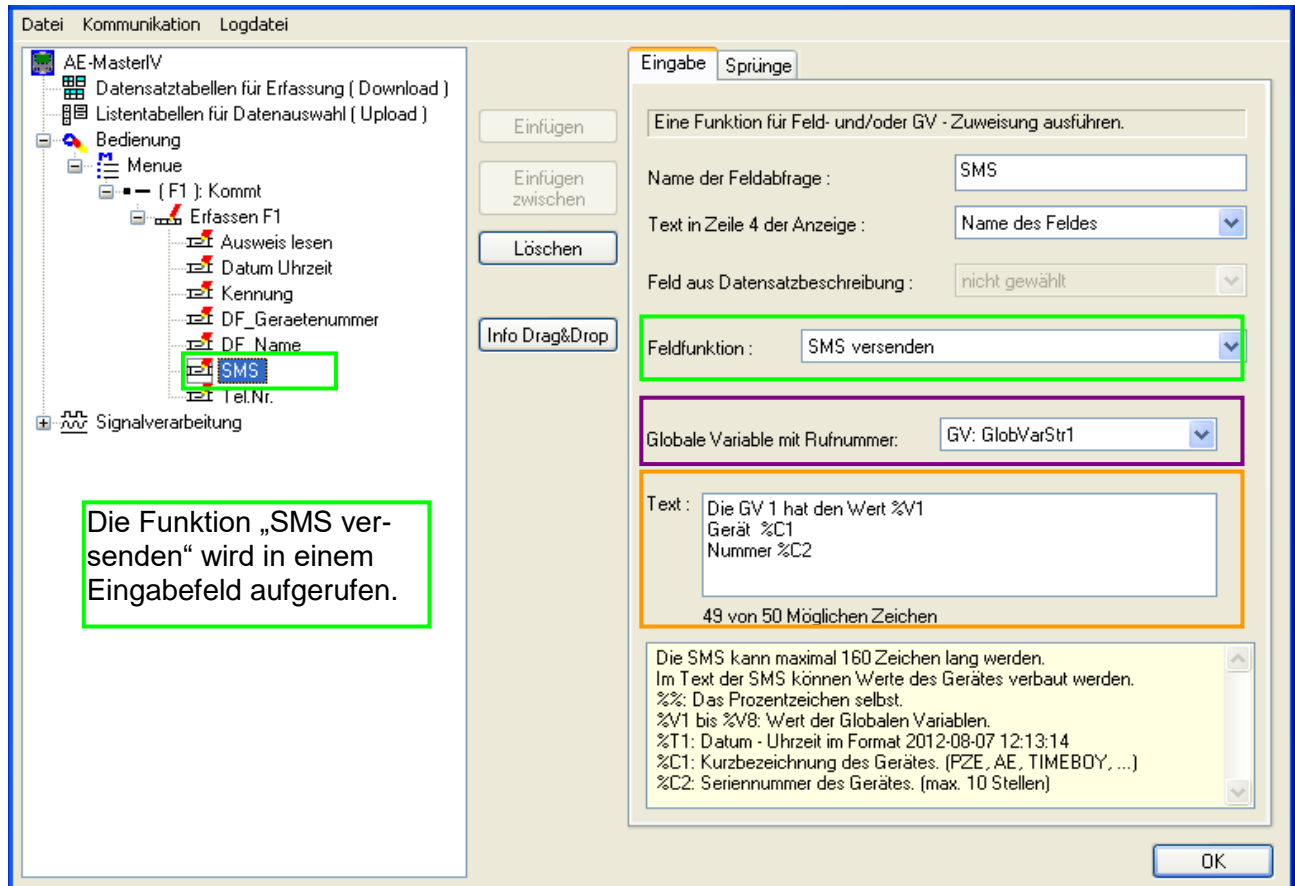
Werden Datensätze über HTTP versendet, können die Feldinhalte verschlüsselt übertragen werden. Die Datenfelder des Datensatzes werden dann mittels einer RC4-Verschlüsselung chiffriert. Die so verschlüsselten Zeichen werden in Hexadezimaldarstellung als Feldinhalt übertragen.

Mehr zum Thema Verschlüsselung der Daten beim Versenden über HTTP finden Sie in Handbuch DatafoxStudioIV unter dem Kapitel [„Konfiguration > Verschlüsselung der Datenfelder beim Versand per HTTP“](#).

5.7.9. Kommunikation per SMS

5.7.9.1. SMS versenden

Datafox MasterIV-Geräte, die mit einem GPRS-Modem ausgestattet sind, sind nun 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).

5.7.9.2. 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:

- ▶ 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.

Name	Wert
PHONE	*99**1#
GPRS	internet.eplus.de
USER	blau
PASSWORD	blau
HOST	www.datafox.de
PORT	80
HTTPSEND	GET /httpdemo/getdata.php?
ALIVE	0
HTTPTIMEOUT	10000
HTTPTYPE	1.1
SIMPIN	0
SIMPUK	0
ROAMING	1
RESETTRIGGER	32
ATTACH	32
ERRORLEVEL	0
HTTP	0
KEY	
DNS1	130.149.17.5
SMSKEY	F3F0D9E9C4D7B33041EBF2B82683DFE8EA7129ABD

Erstellung des Wertes für die Systemvariable MOBILE.SMSKEY

Passwort :

Wert für SysVar : F3F0D9E9C4D7B33041EBF2B82683DFE8EA7129ABD

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.

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.

Beispiele:

- a) service=1
- b) service=1&host=www.datafox.de
- c) service=1&host=123.123.123.123
- d) service=1&host=www.datafox.de&port=4711

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.

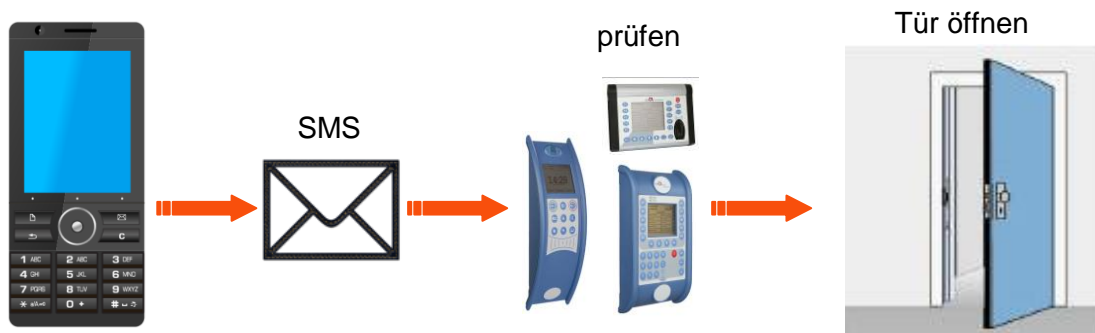
Eine Eingabekette in der Signalverarbeitung starten

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

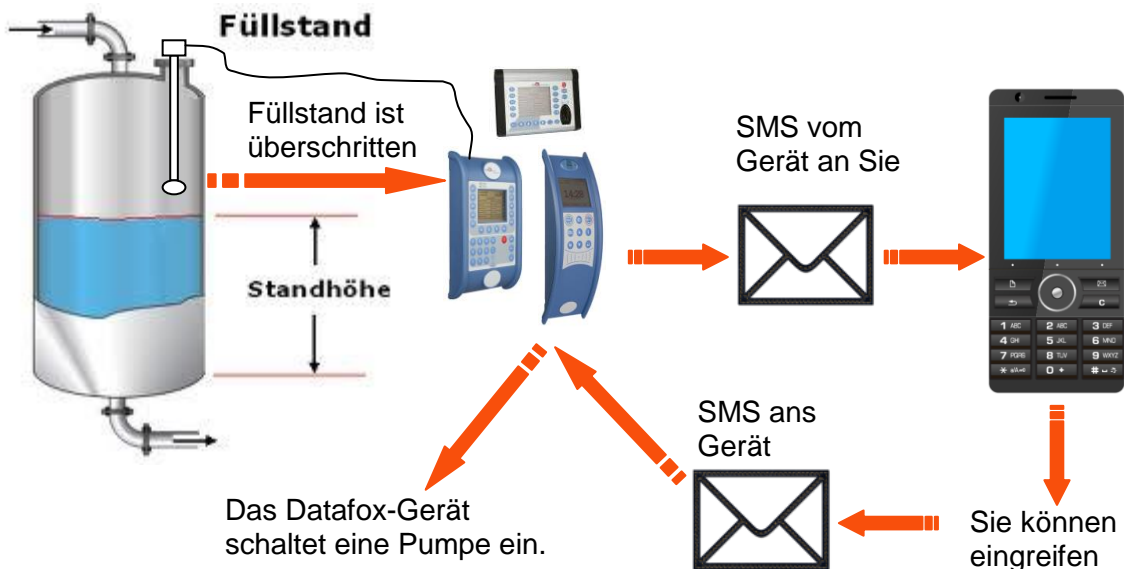
Die Möglichkeiten, die sich dadurch ergeben, sind sehr zahlreich.
 Beispiele:

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.

5.8. Anschluss der Zutrittskontrolle

5.8.1. 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.

ZK-MasterIV



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



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

50 x 50 x 43 mm (BxHxT)



Der RELINO 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.

IO-Box



51 x 48 x 22 mm (LxBxH)

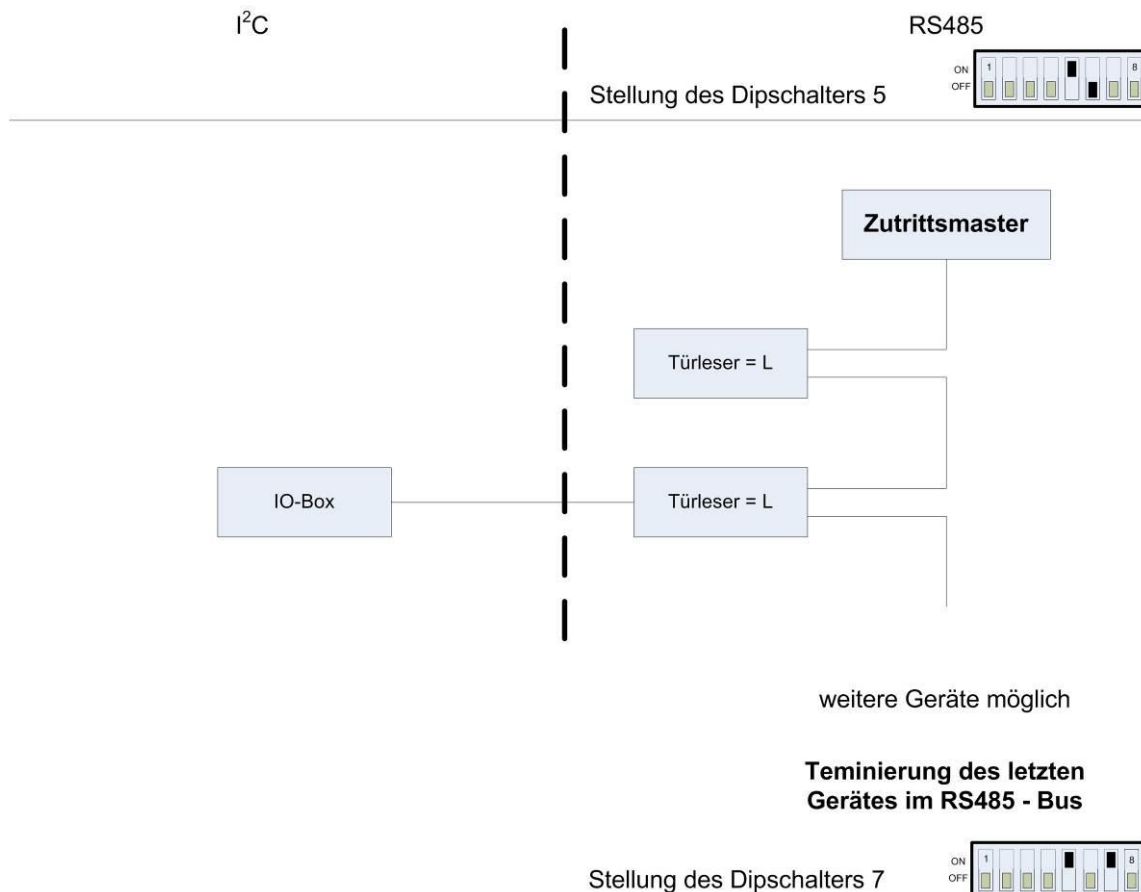
Die IO-Box als Zubehör für den RFID-Wandler bzw. RELINO Leser besitzt zwei digitale Eingänge und zwei digitale Ausgänge. Als Schnittstelle kommt der I 2 C Bus zum Einsatz.

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.

5.8.1.1. 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>

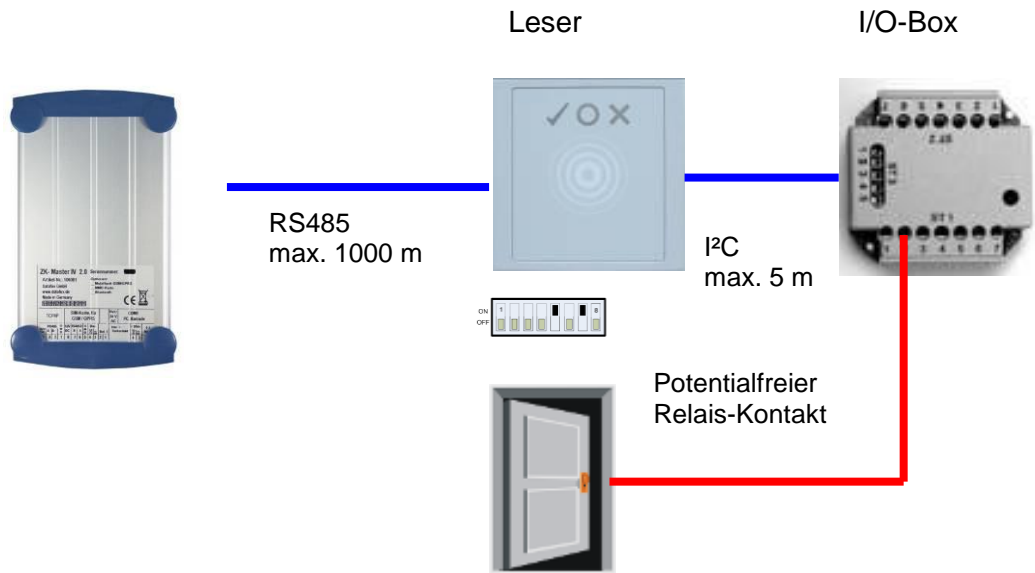
In den PHG Dokumenten zu den einzelnen Modulen, wird die Anschlussbelegung und Konfiguration über die Dip-Schalter beschrieben. Um mit dem ZK-MasterIV eine Zutrittskontrolle durchzuführen, muss die Option „Zutritt“ integriert sein (Datafox Artikel-Nr. 105201). Die folgende Grafik zeigt die Anschlussmöglichkeiten der PHG-Geräte an einen AE-MasterIV 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“.

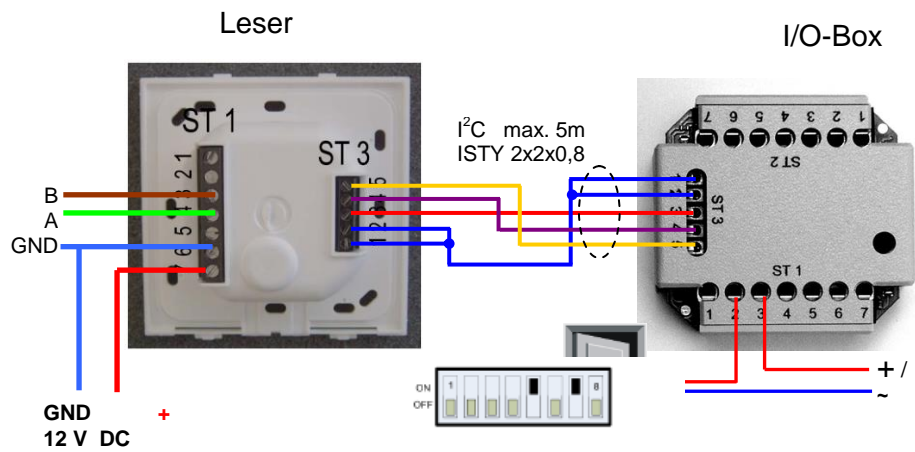
Wenn zusätzlich ein Türöffner über ein Relais gesteuert werden soll, muss eine IO-Box zum Einsatz kommen. Mit jeder IO-Box stehen zwei digitale Ausgänge in Form von Relais zur Verfügung.

Anschlussbeispiel eine Tür mit I/O-Box:

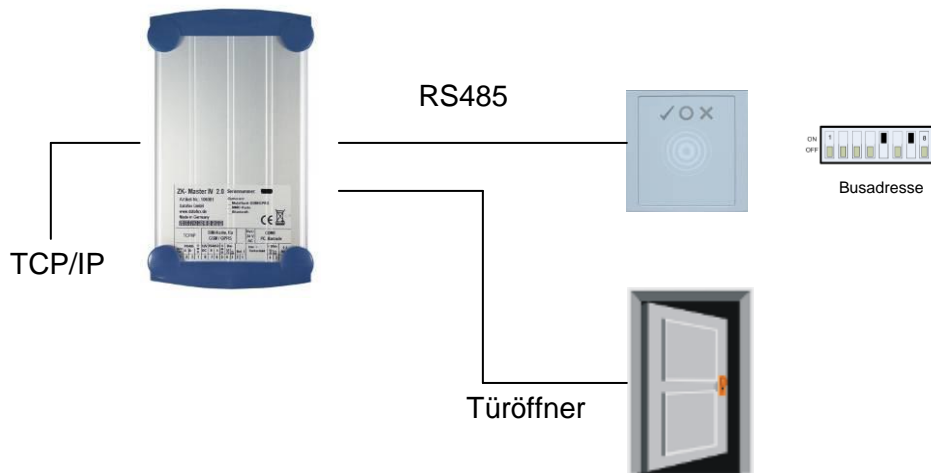


Stecker ZK-Master IV

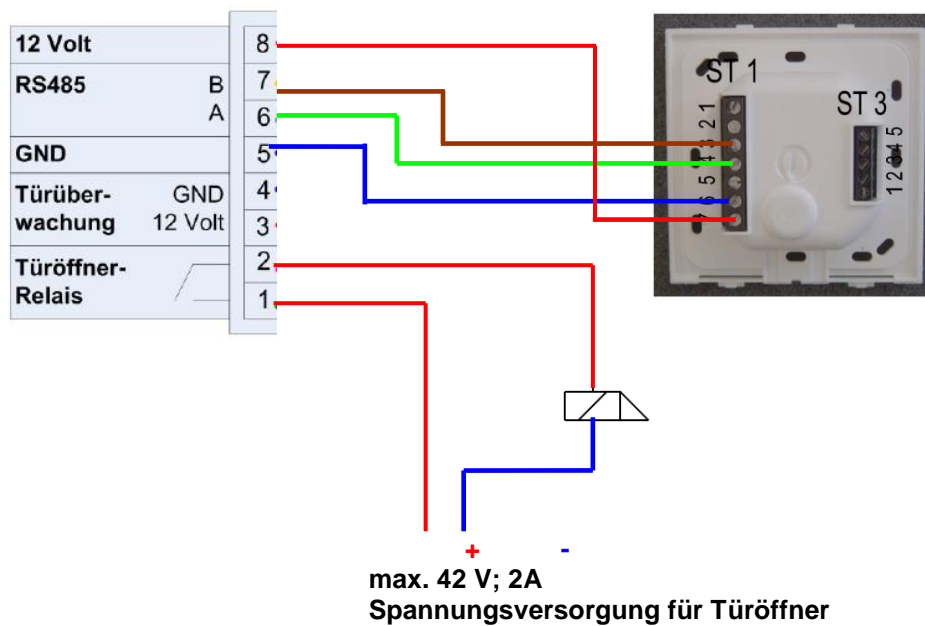
12 Volt	8
RS 485 A	7
RS 485 B	6
GND	5
digital GND	4
1 in + 12 V	3
no Schließer	2
com	1
nc Öffner	0



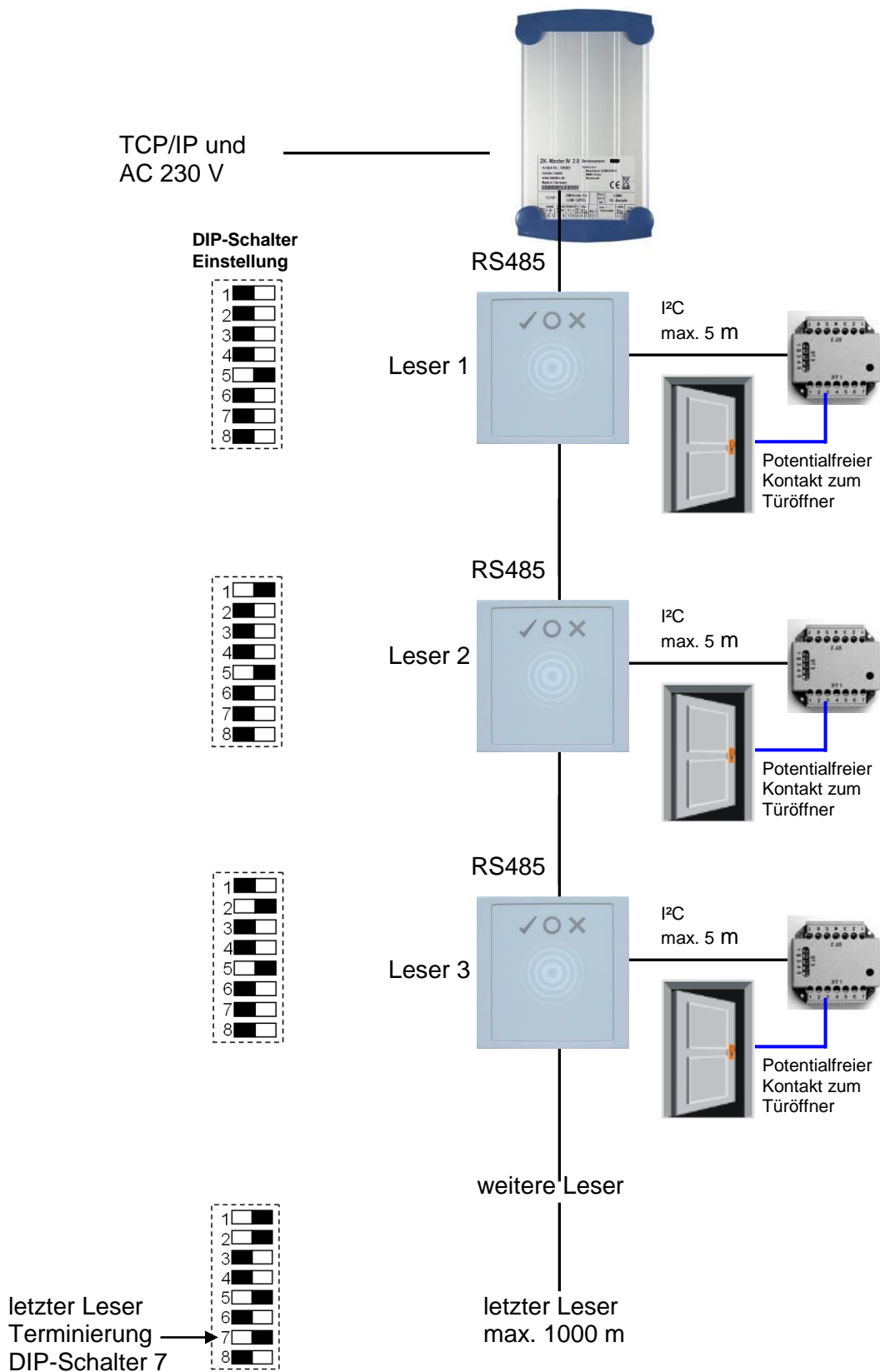
Anschlussbeispiel eine Tür ohne I/O-Box:



Verdrahtungsplan



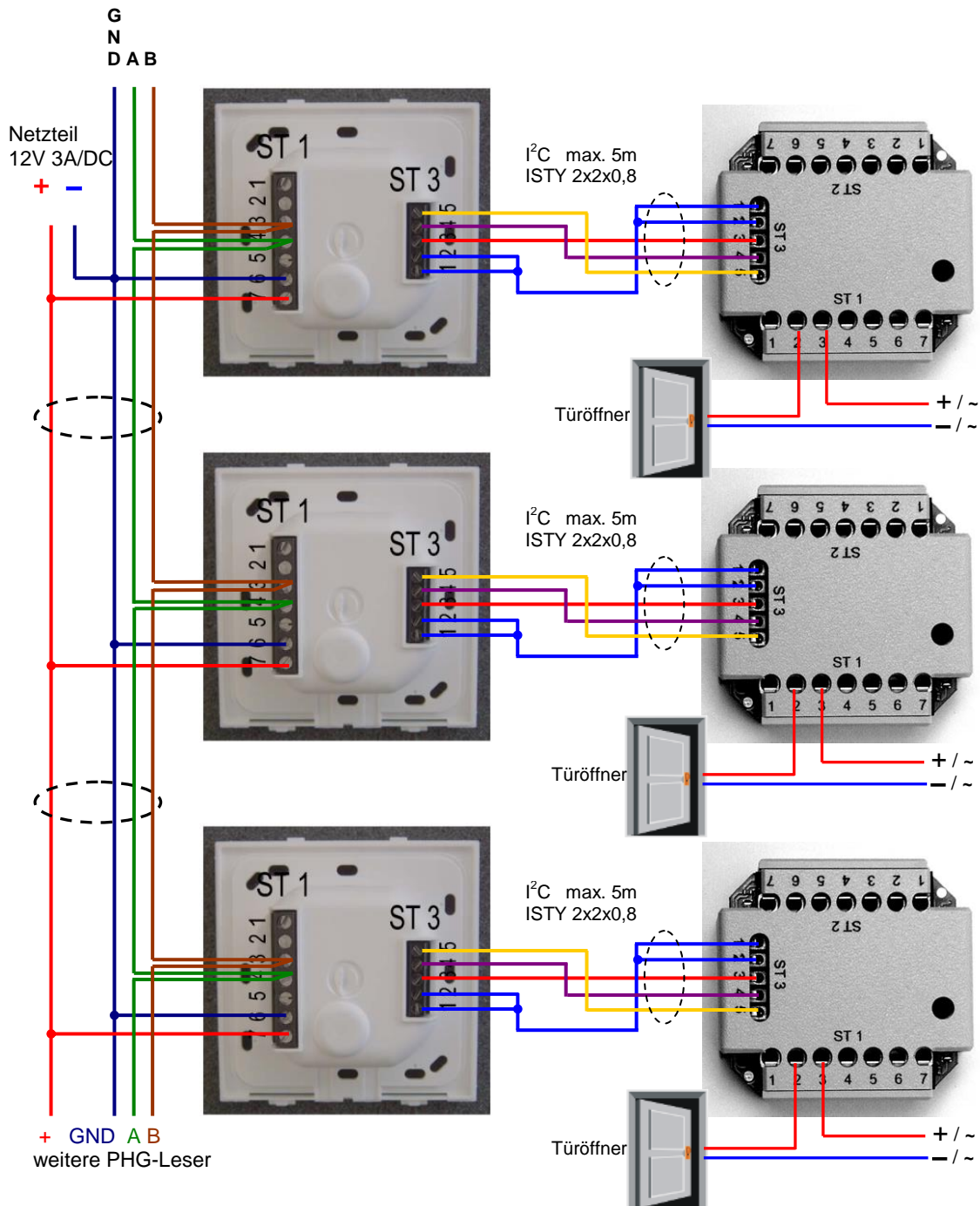
Schematischer Aufbau der RS485 Busverkabelung einer Zutrittskontrolle



Verdratungsplan meherer PHG-Leser:

Stecker ZK-Master IV

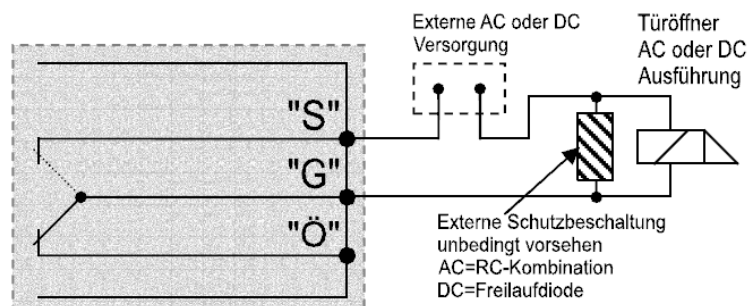
12 Volt		8
RS 485	A	7
	B	6
GND		5
digital	GND	4
	+ 12 V	3
no Schließer		2
com		1
nc Öffner		0



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

Anschlussklemmen der IO-Box:

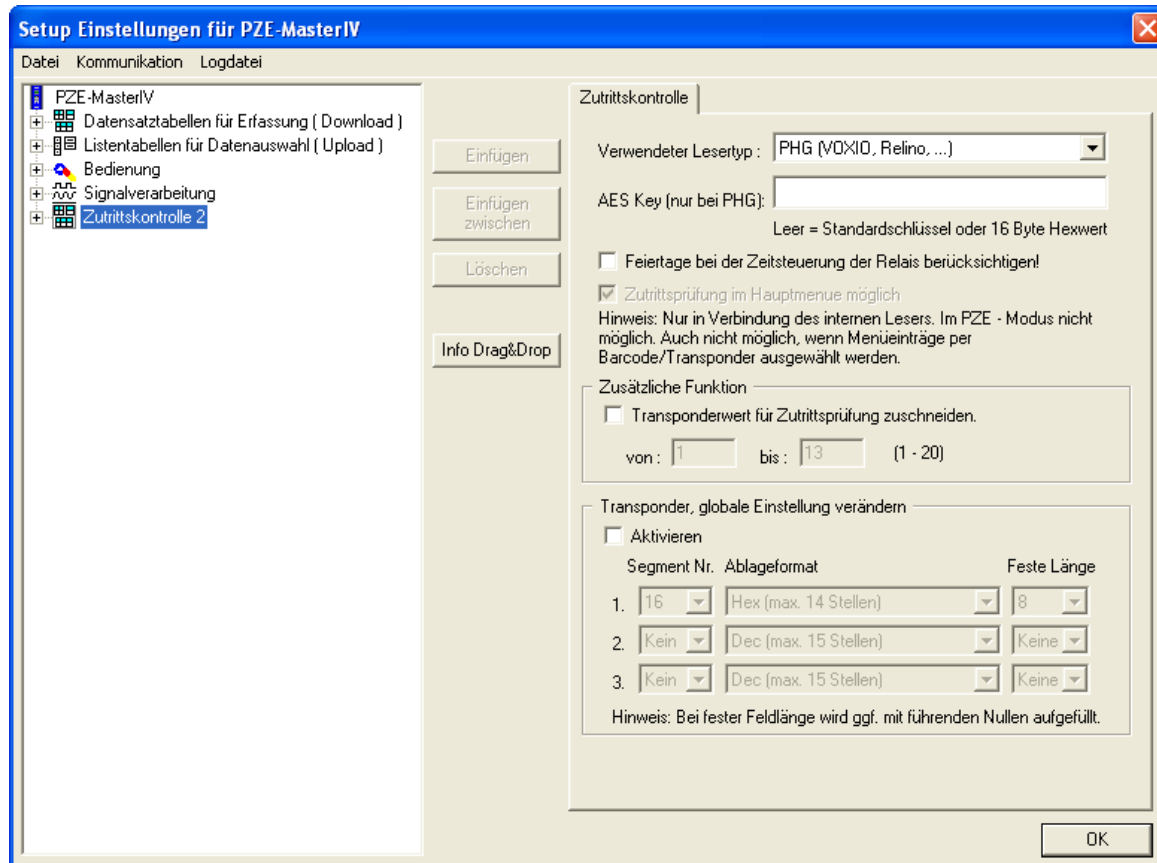
Anschluss (ST1,2,3)	Klemme Nr.	Beschreibung
ST1	1	Relais 1 → „Ö“ Öffner
	2	Relais 1 → „G“ Gemeinsamer
	3	Relais 1 → „S“ Schließer
	4	NC
	5	NC
	6	Eingang 2 Signal
	7	Eingang 2 GND
ST2	1	Relais 2 → „Ö“ Öffner
	2	Relais 2 → „G“ Gemeinsamer
	3	Relais 2 → „S“ Schließer
	4	NC
	5	NC
	6	Eingang 1 Signal
	7	Eingang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



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

5.8.1.2. 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.

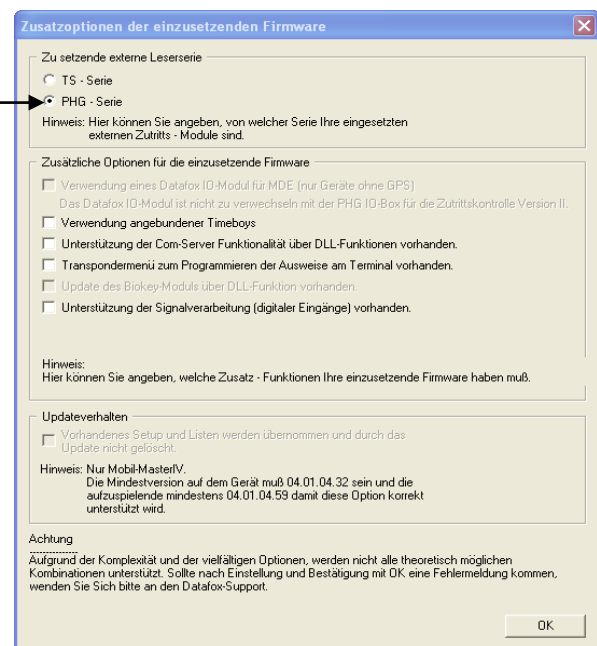
PHG-Leser haben im Gegensatz zu den GIS-Lesern immer 2 digitale Eingänge und einen Sabotagekontakt. Die Firmware betrachtet Eingang 1 und Eingang 2 als normalen Eingang mit der Nummer 1 und 2 den Sabotagekontakt als Nr. 3. Der Sabotagekontakt ist im Leser integriert. Der PHG-Leser verfügt nicht über 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	1	011	1	1	0	IO-Box an I²C-Bus
4	1	020	2	2	0	Leser an RS485 (LTM)
5	1	021	2	2	0	IO-Box an I²C-Bus

5.8.2. 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.

ZK-MasterIV



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:

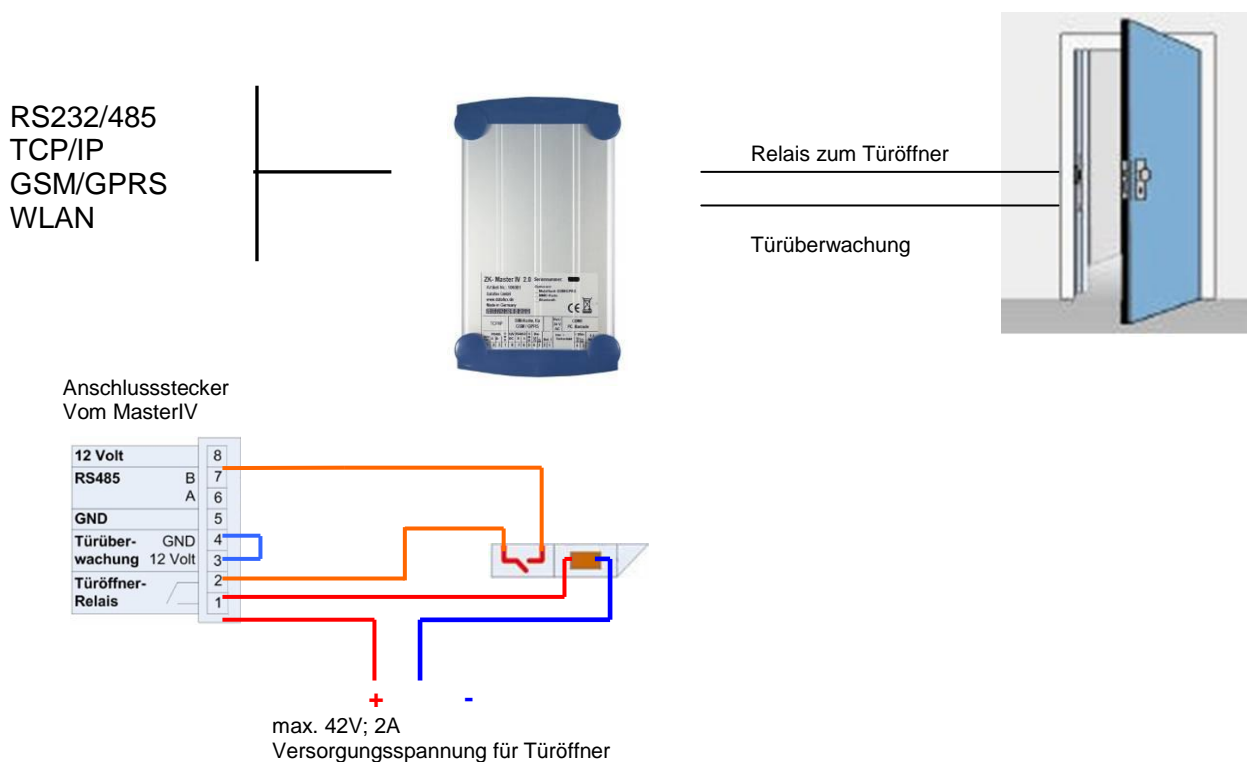
Die einzelnen Module werden an einen Bus angeschlossen. Hierbei legt der Dippschalter 5 fest, ob diese über RS232 oder RS485 kommunizieren sollen.

5.8.2.1. Aufbau und Installationsvarianten

Nachfolgend werden die verschiedenen Aufbaumöglichkeiten dargestellt. Als Referenzgerät auf den Bildern wird der PZE-MasterIV verwendet. Die Varianten für den Aufbau sind für alle MasterIV Geräte gleich.

Eine Tür ohne separaten Leser

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



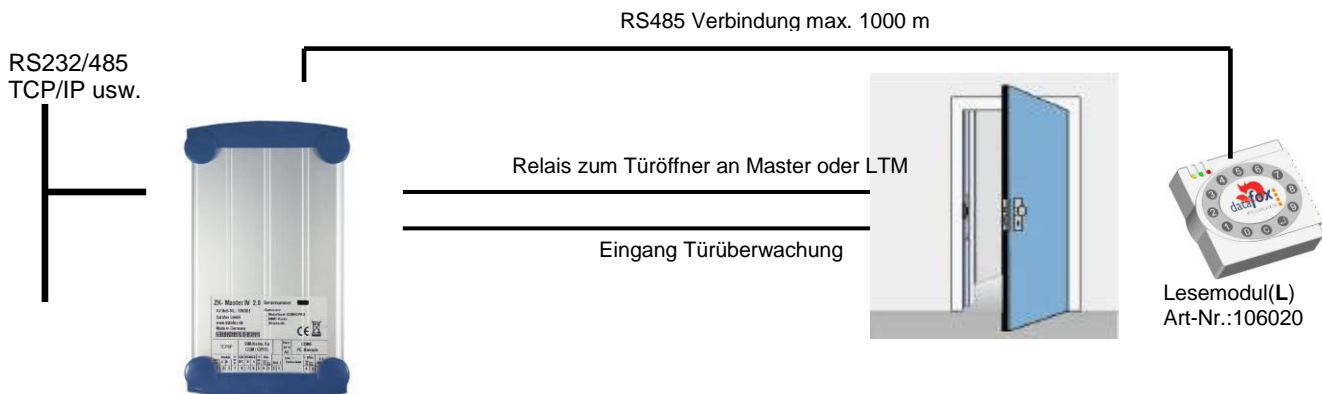
Achtung:

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

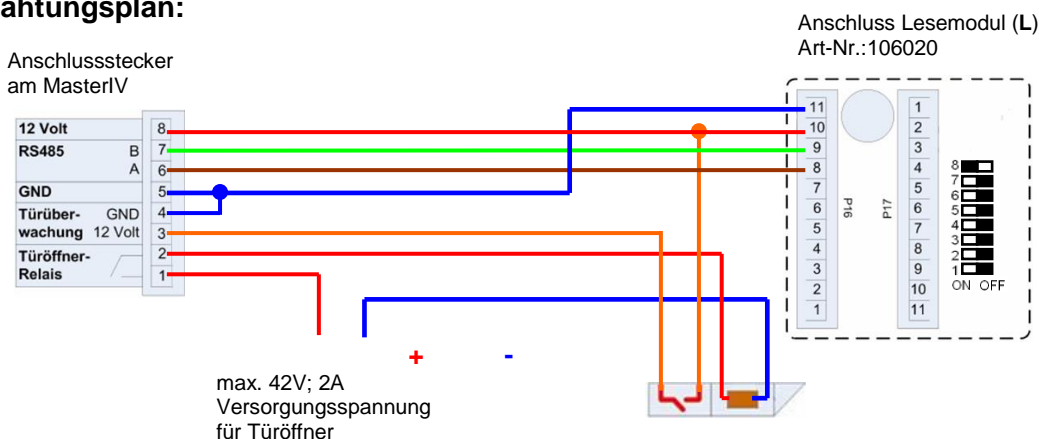
Übersichtsplan:



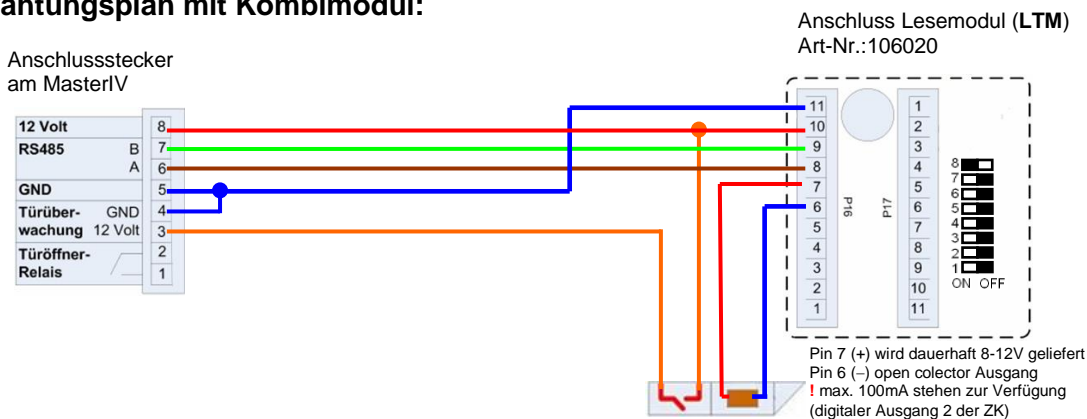
Diese Variante wird in der Praxis sehr oft gefordert und kann mit der oben

gestellten Lösung sehr leicht und kostengünstig umgesetzt werden.

Verdrahtungsplan:



Verdrahtungsplan mit Kombimodul:



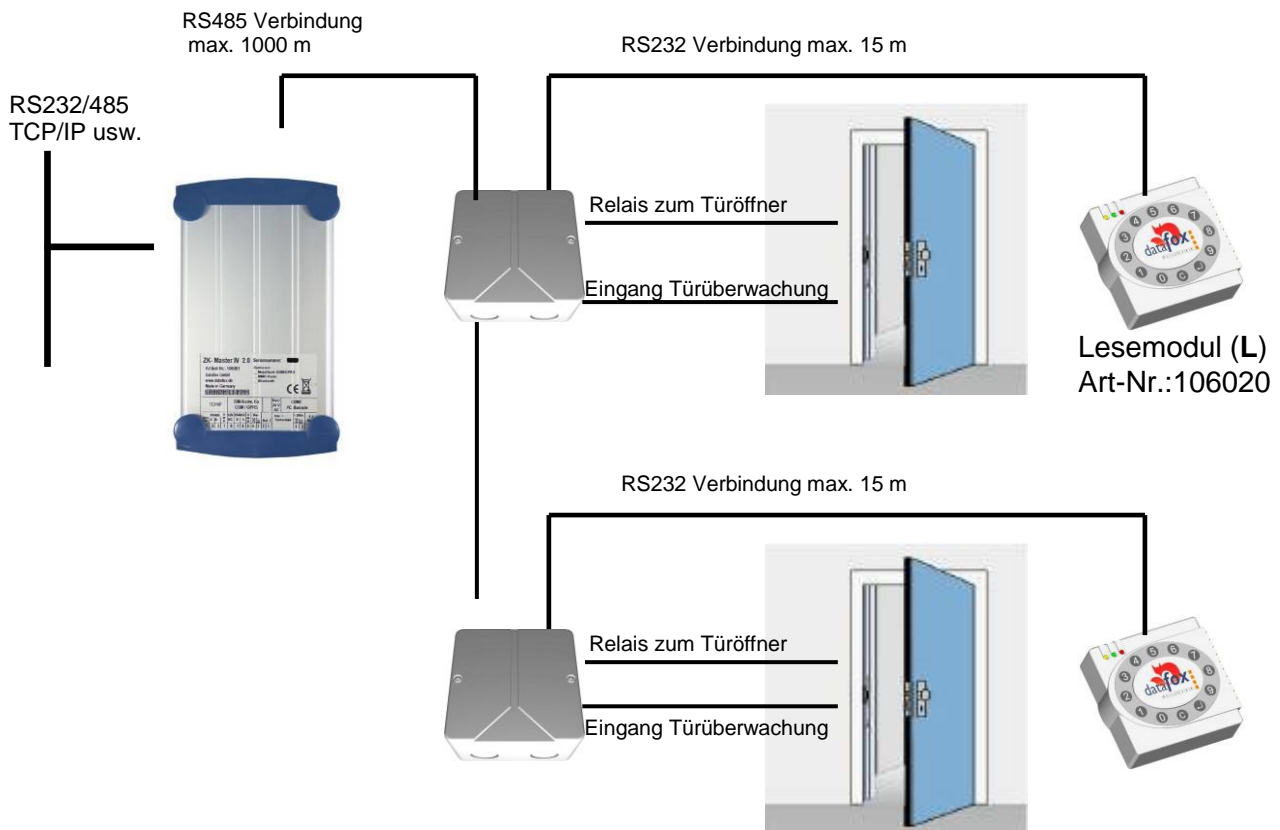
Entsprechende Reader Tabelle

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.

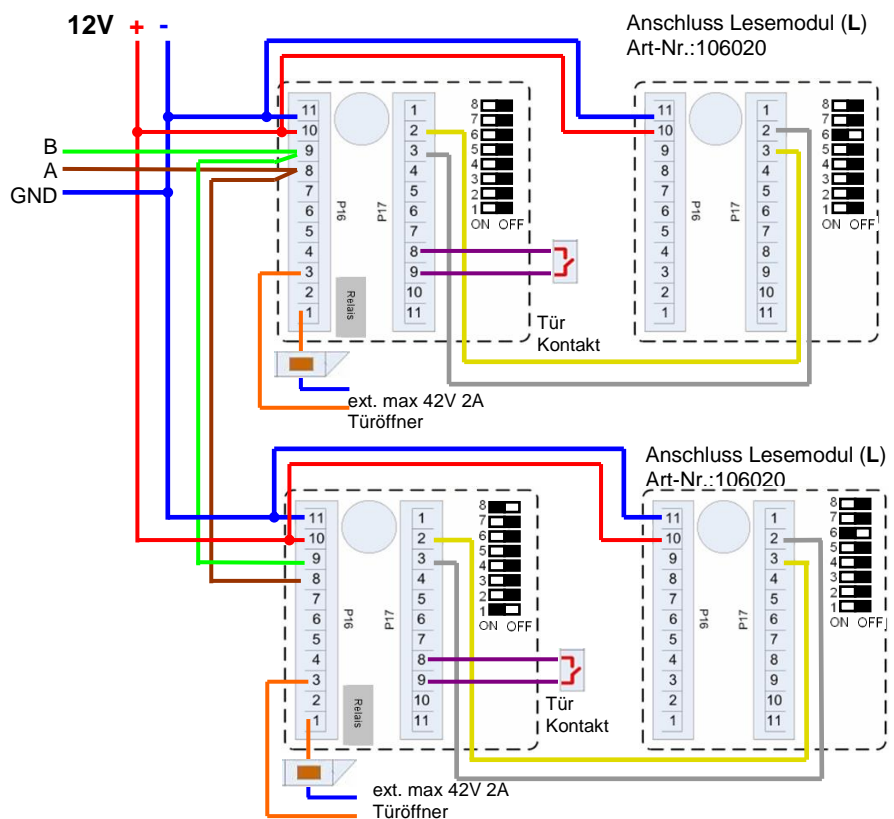
Übersichtsplan:



Verdrahtungsplan:

Stecker ZK-Master IV

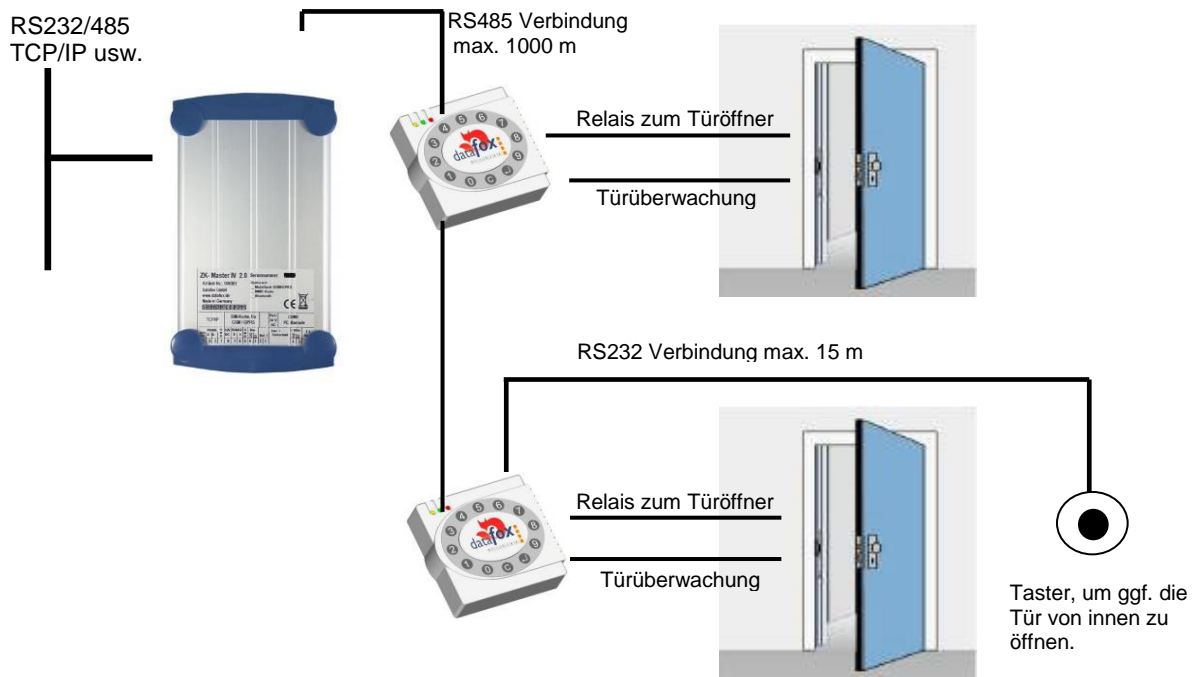
12 Volt	8
RS 485 A	7
RS 485 B	6
GND	5
digital GND	4
1 in +12 V	3
no Schließer	2
com	1
nc Öffner	0



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.

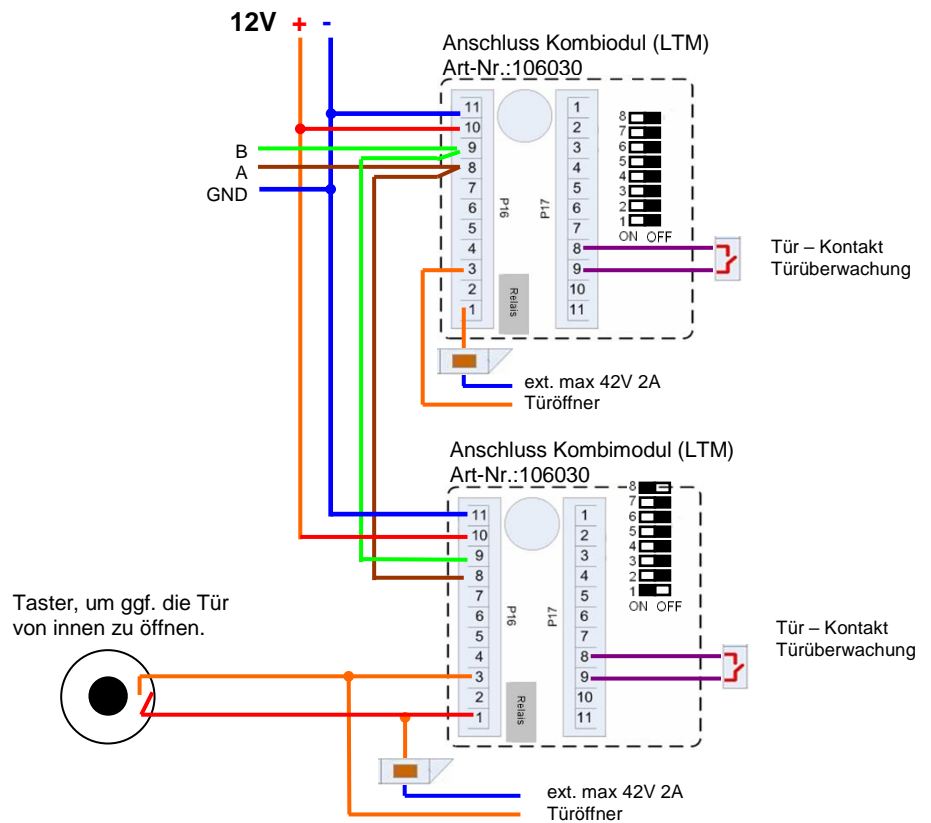
Übersichtsplan:



Verdrahtungsplan:

Stecker ZK-Master IV

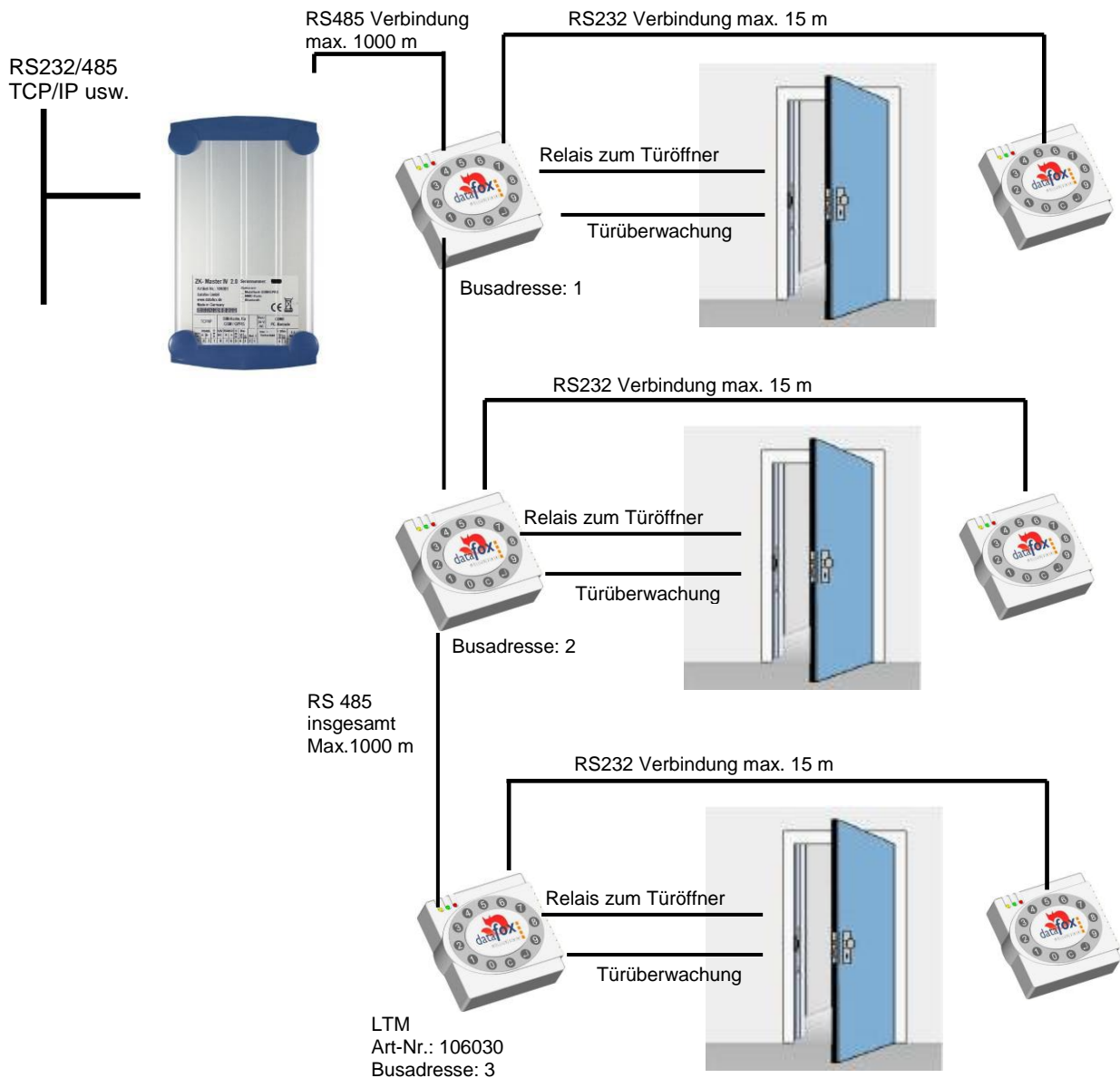
12 Volt	8
RS 485 A	7
RS 485 B	6
GND	5
digital GND	4
1 in + 12 V	3
no Schließer	2
com	1
nc Öffner	0



Schleusenfunktion mit RS485 - Bus

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

Übersichtsplan:



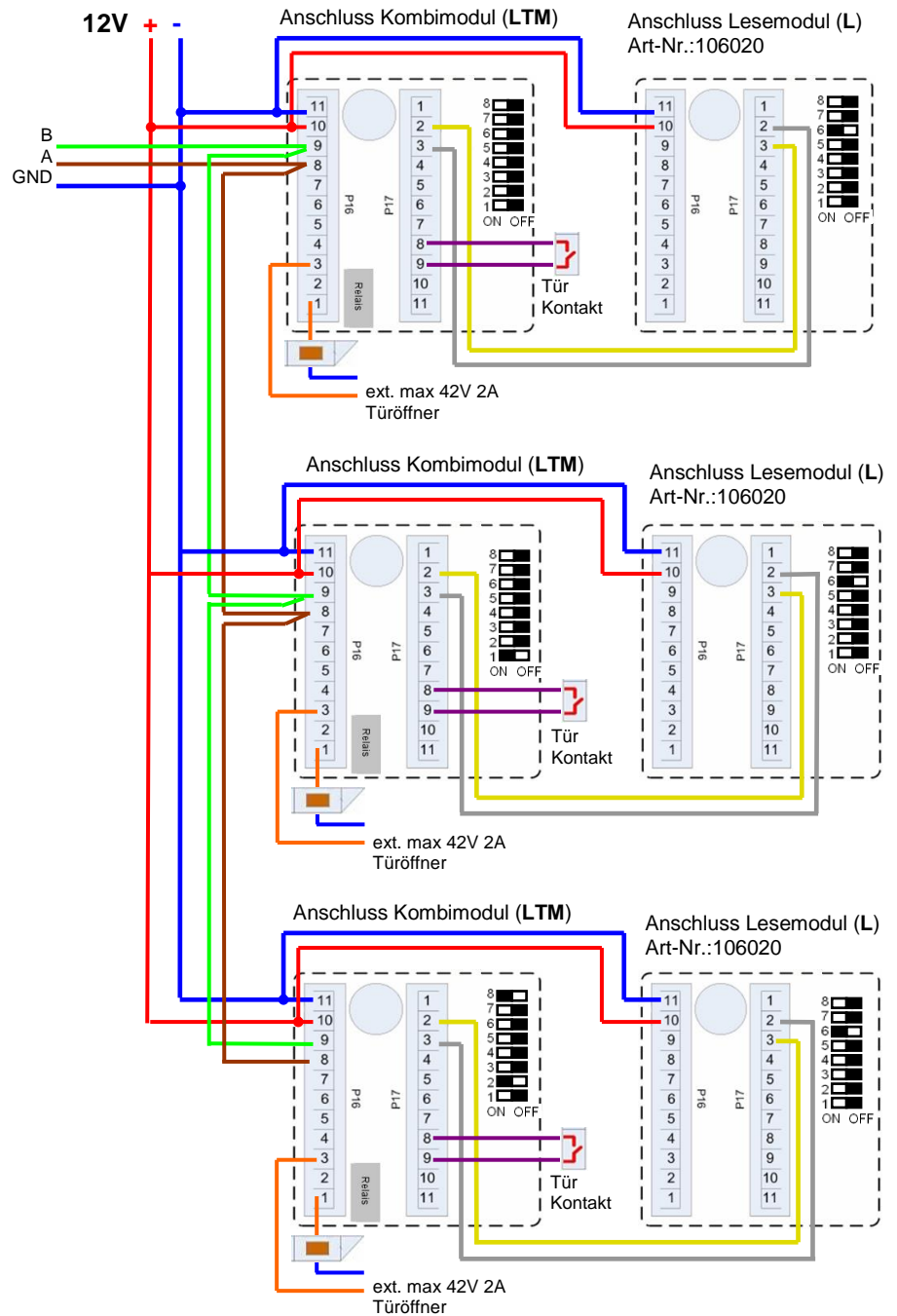
Entsprechende Readertabelle:

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:

Stecker ZK-Master IV

12 Volt	8
RS 485 A	7
RS 485 B	6
GND	5
digital GND	4
1 in +12 V	3
no Schließer	2
com	1
nc Öffner	0



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.

5.8.2.2. Anschluss der TS-Leser

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

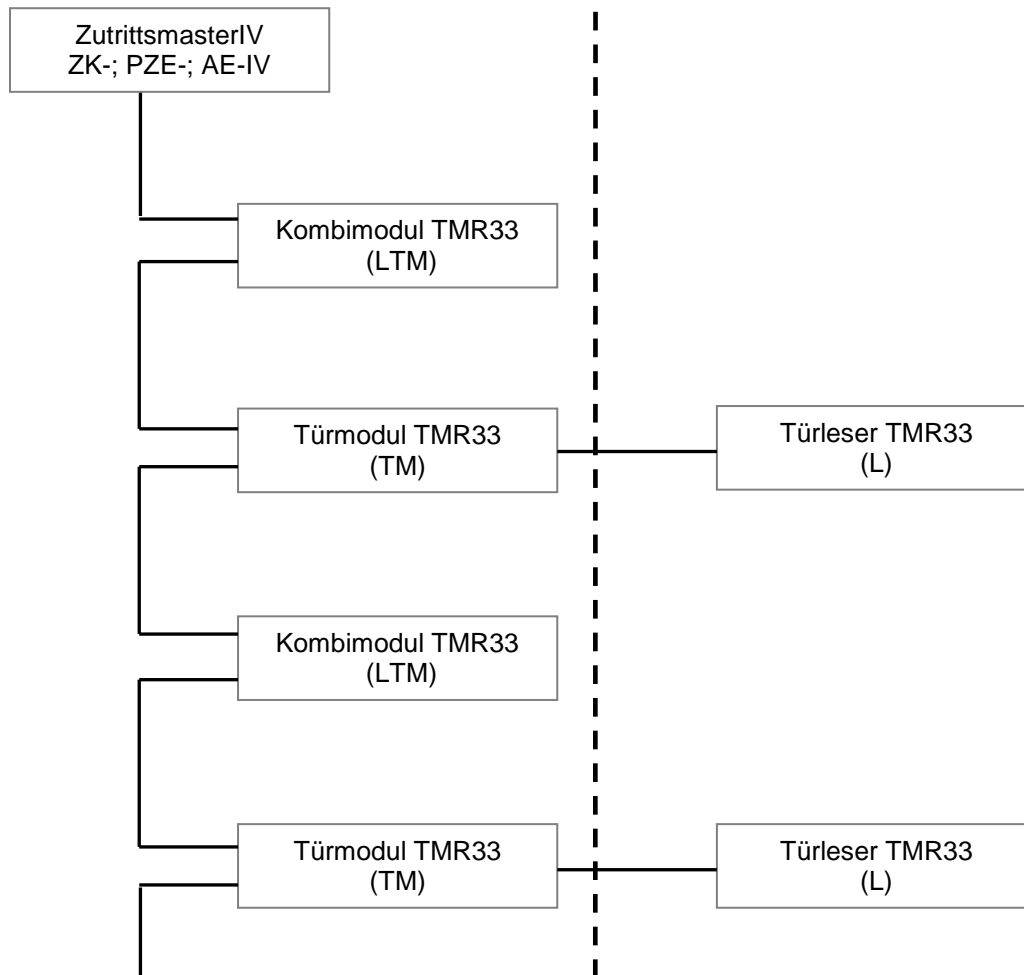
RS 485

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:

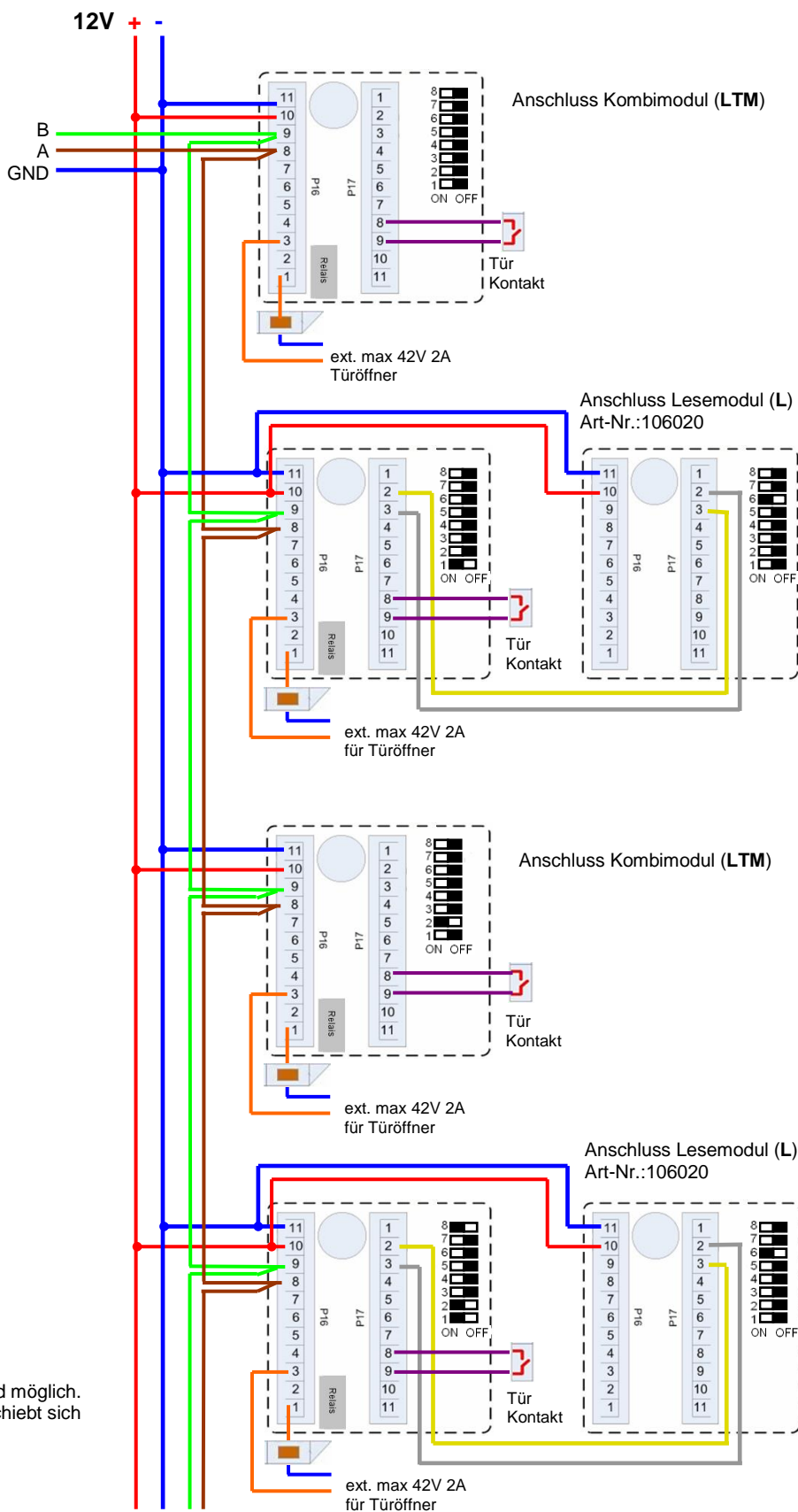


Die Dip-Schalter 1-5 dienen der Bus-Konfiguration. Mit ihnen wird die Bus-Nr. des Gerätes eingestellt. Der Dip-Schalter 1 in der Position „ON“ und 2-5 in der Position „OFF“ entspricht der Bus-Nr „1“. Der Dip-Schalter 1 und 2 in der Position „ON“ und 3-5 in der Position „OFF“ entspricht der Bus-Nr „3“.

Verdrahtungsplan:

Stecker ZK-Master IV

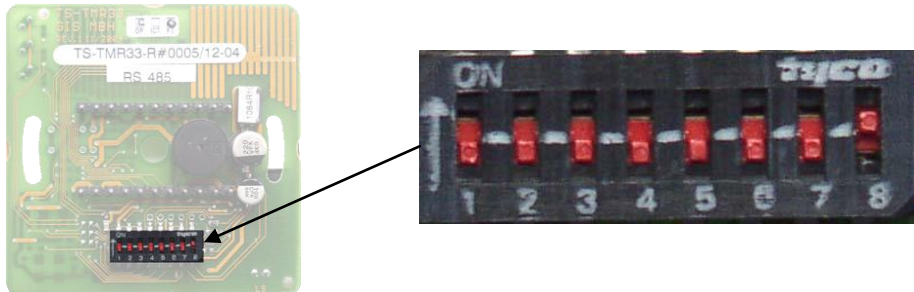
12 Volt		8
RS 485	A	7
	B	6
GND		5
digital	GND	4
1 in	+ 12 V	3
no Schließer		2
com		1
nc Öffner		0



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.					

Berechnungsvorschrift für die Spannungsversorgung der Module

Beim Einsatz von Datafox Zutrittslesern und Türmodulen (TS-TMR33-Module), ist vor der Errichtung eines RS485-Netzwerkes für die Zutrittskontrolle der notwendige Leitungsquerschnitt zu berechnen. Der Spannungsabfall darf im gesamten Bus nicht größer sein als 4 V. Dabei ist zu beachten, dass mit einem Datafox Gerätenetzteil als Spannungsquelle max. 16 Module (8 im RS485 Bus und 8 über RS232 Stichleitung) gespeist werden können.

Max. Stromverbrauch der einzelnen Module:

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

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 mm²

I = Stromstärke

l = Leitungslänge in m

k = Leitfähigkeit für Kupfer $56 \frac{m}{\Omega \cdot mm^2}$

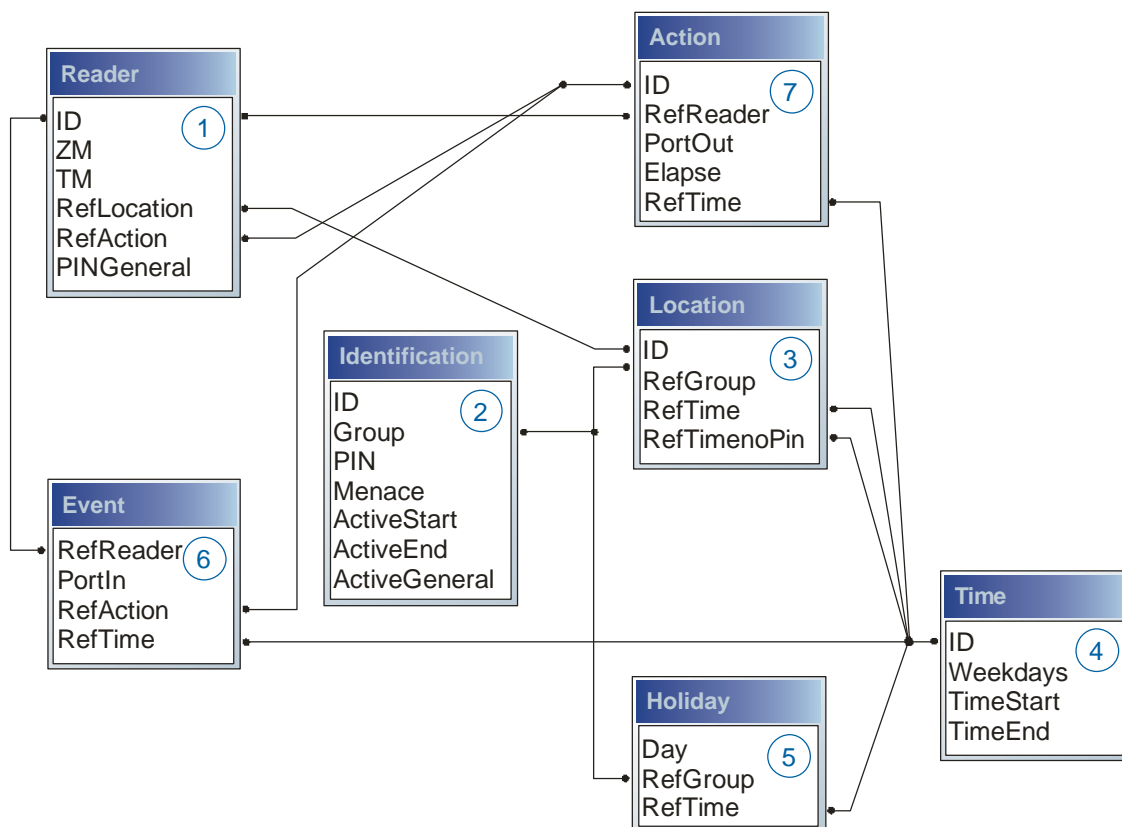
U_v = Spannungsabfall max. 4 V

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

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

Konfiguration

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



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

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

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

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

Feiertagssteuerung

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

Beispiel:

Action

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

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“ werden nur die ersten 32 Einträge bei einer Zeitsteuerung unterstützt.

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 AE-MasterIV 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	TimeEnd	TimeEnd
3	12345	10:00	00:00
4	12345	16:00	00:00
5	1234567	07:00	19:00

Action.txt

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

5.8.3. Beschreibung der Tabellen für die Zutrittskontrolle 2

Bezeichner	Datentyp	Länge	Beschreibung
ID	Nummer (int)	4	Eindeutiger Schlüssel (Wert>0) der Reader Tabelle.
ZM Bus ID Nummer	Nummer (int)	4	Enthält in unserem Beispiel die Nummer 1. Existieren in einem Zutrittssystem mehrere PZE-MasterIV, können diese in einem Tabellenzusammenhang abgebildet werden und es ist nicht nötig für jeden PZE-MasterIV einen separaten Strang zu pflegen.
TM	Nummer (int)	3	Enthält zwei Informationen in einer Zahl. 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 als Stich.
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 Reader (Liste aller im System installierten Geräte)

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. Bitte beachten Sie, dass die Pin nicht mit einer 0 beginnen darf. 0815 z.B. wäre ungültig!!
Menace	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. 2007-07-12 = 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) 3 = Zutritt nur über PIN Eingabe 8 = Generelle Berechtigung (mit PIN-Abfrage) 9 = Generelle Berechtigung (keine PIN-Abfrage)

Tabelle Identification (Liste aller bekannten Ausweise)

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 Holiday (Festlegung von Sperrtagen, Feiertage und Betriebsurlaub)

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 zugriffsberechtigte Gruppe. Alle Ausweise dieser Gruppe haben zu diesem Raum Zutritt.
RefTime	Nummer (int)	4	Das Zeitmodell, in welchem berechtigte Personen Zutritt erhalten. (0 = wird nicht verwendet)
RefTimeNoPin	Nummer (int)	4	Das Zeitmodell, zu dem eine zusätzliche PIN nicht eingegeben werden muss (in Stosszeiten, etc.).

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

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

Bezeichner	Datentyp	Länge	Beschreibung
RefReader	Nummer (int)	4	Modul (Türmodul oder Master) auf dem sich der digitale Eingang befindet.
PortIn	Nummer (int)	1	Nummer des digitalen Eingangs auf dem Modul.
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 = wird nicht verwendet)

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

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 (int)	1	Gibt die Nummer des Ausgangs auf dem Modul an.
Elapse	Nummer (int)	3	Die Dauer, für die das Relais geschaltet wird (0 = dauerhaft). 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!

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

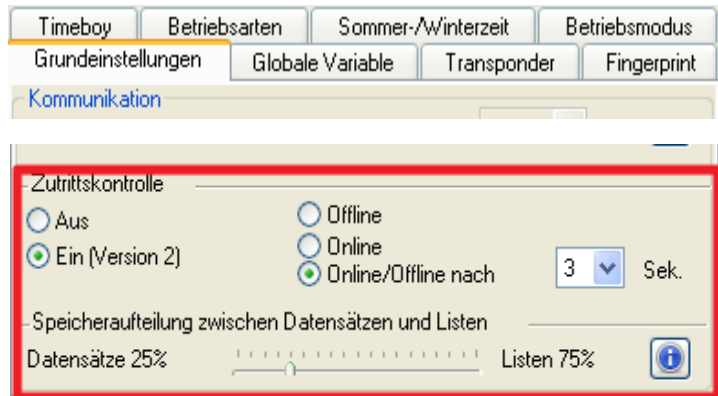
5.8.4. Onlinefunktionen der Zutrittskontrolle

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.



5.8.4.1. 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`

<code>Master_ID=1</code>	Master-ID
<code>Modul_ID=010</code>	Busadresse des Lesers / TM
<code>Ausweis_Nr=2058</code>	Ausweisnummer
<code>Status=34</code>	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`

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

<code>access=010</code>	Busadresse, auf der die Aktion durchgeführt werden soll
<code>module=010</code>	Busadresse, auf der die Aktion durchgeführt werden soll
<code>master=1</code>	Bus-Strang auf dem geschaltet werden soll
<code>mask=5</code>	Rote LED + Buzzer
<code>type=1</code>	einschalten
<code>duration=2</code>	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=	000	
oder	010	Der Wert der Zeichenfolge, muss dem Format des Feldes "TM" der "Reader" Liste folgen. Er muss demnach immer 3 Ziffern umfassen.
module=	011	
Funktion für 1x Bus RS485	...	
	081 usw.	
	1-3	Id für den RS485 Bus ZK, Beschreibt den ZK-Bus-Strang. RS485 Bus ID 1
master =	1	RS485 Bus ID 2 usw.
	2	„ master “ muss gemeinsam mit „ module “ eingesetzt werden und ersetzt damit „ access “
	1 / 0	Bei gesetztem Bit, wird der Buzzer angesprochen.
	2 / 1	Bei gesetztem Bit, wird die grüne LED angesprochen.
	4 / 2	Bei gesetztem Bit, wird die rote LED angesprochen.
	8 / 3	Bei gesetztem Bit, wird das 1 Relais angesprochen.
mask	16 / 4	Bei gesetztem Bit, wird das 2 Relais angesprochen.
	32 / 5	Bei gesetztem Bit, wird das 3 Relais angesprochen.
	64 / 6	Bei gesetztem Bit, wird das 4 Relais angesprochen.
	128 / 7	Bei gesetztem Bit, wird das 5 Relais angesprochen.
	256 / 8	Bei gesetztem Bit, wird das 6 Relais angesprochen.
	Unbenutzt. Bitte immer auf 0 setzen.
	0	Aus
type	1	Ein
	2	Wechsel (600ms an, 600ms aus)
	3	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.



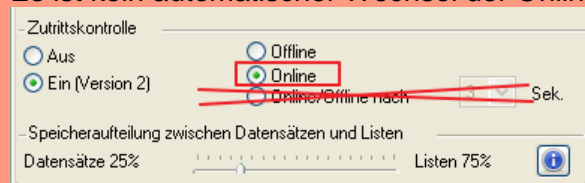
Hinweis:

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.

5.8.4.2. 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.
http://www.datafox.de/software-de.html?file=tl_files/Datafox_Devices/Downloads_Geraete_Zubehoer/MasterIV-Software/Datafox_SDK_Windows.zip

5.8.5. Funktionserweiterung für die Zutrittskontrolle 2

5.8.5.1. 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:

5.8.5.2. Beispiele

Beispiel Werkstatt

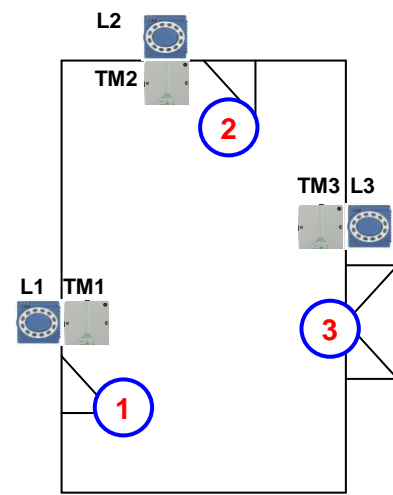
Der Hausmeister kommt am Morgen um 7.00 Uhr und nutzt dabei einen Eingang **1**.

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

> weiter wird das Tor **3** für das Öffnen mit einem Taster über einen Schließerkontakt bis 16.00 Uhr freigegeben, > und der Eingang **2** bleibt bis 16.00 Uhr 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.

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

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	2	1	-1	3	0	Türöffnung wird zurückgenommen.
1000	40	0	4	1	-1	5	0	Torfreigabe wird 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 zurückgenommen.
2000	40	0	6	1	-1	7	0	Torfreigabe wird zurückgenommen.
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	

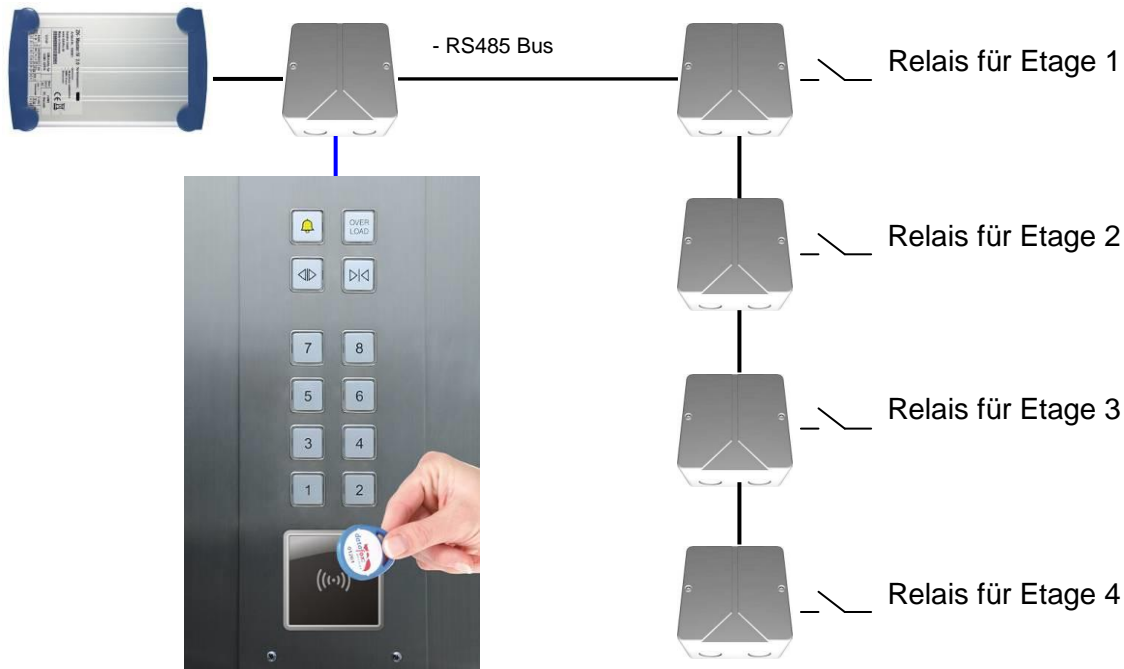
Tabelle Identification

ID	Group	Pin	Menace	ActiveStart	ActiveEnd	Active	Beschreibung
1111	10	0	0	2005-01-01	2015-12-31	1	Werkstattleiter
2222	20	0	0	2005-01-01	2015-12-31	1	Angestellte
3333	30	0	0	2005-01-01	2015-12-31	1	Hausmeister
4444	40	0	0	2005-01-01	2015-12-31	1	Hausmeister 2, Transponder für Schließung

Beispiel Aufzugsteuerung

Ziel ist es, dass 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 befindet sich auf der Kabine.



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

Tabelle Reader

ID	ZM	TM	RefLocation	RefAction	PinGeneral	Beschreibungstext
1	1	010	100	0	0	Türmodul an RS485 mit Relais für die Etage 1
2	1	020	100	0	0	Türmodul an RS485 mit Relais für die Etage 2
3	1	030	100	0	0	Türmodul an RS485 mit Relais für die Etage 3
4	1	040	100	0	0	Türmodul an RS485 mit Relais für die Etage 4
5	1	320	0	0	0	Mastergerät
6	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	1	0	Gruppe 10 fährt nur in Etage 1.
1000	20	0	2	1	20	2	0	Gruppe 20 fährt nur in Etage 2.
1000	30	0	3	1	20	3	0	Gruppe 30 fährt nur in Etage 3.
1000	40	0	4	1	20	4	0	Gruppe 40 fährt nur in Etage 4.
1000	50	0	1	1	20	5	0	Gruppe 50 darf in die Etagen 1 und 2 fahren.
1000	50	0	2	1	20	5	0	
1000	60	0	1	1	20	5	0	Gruppe 60 darf in die Etagen 1,2,3 und 4 fahren.
1000	60	0	2	1	20	5	0	
1000	60	0	3	1	20	5	0	
1000	60	0	4	1	20	5	0	

Tabelle *Location*

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

Tabelle *Identification*

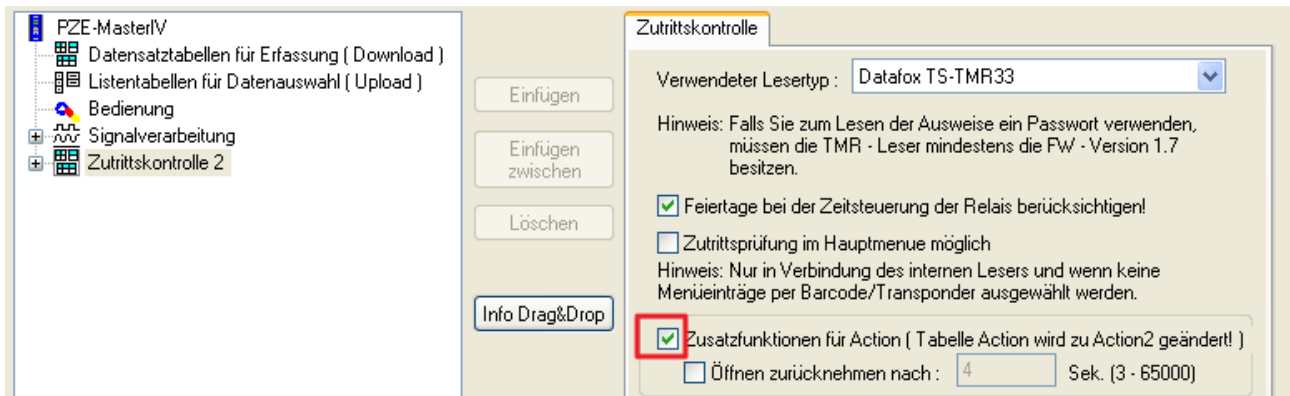
ID	Group	Pin	Menace	ActiveStart	ActiveEnd	Active	Beschreibung
1111	10	0	0	2005-01-01	2015-12-31	1	Mieter Wohnung 1. Etage
1112	10	0	0	2005-01-01	2015-12-31	1	
1113	10	0	0	2005-01-01	2015-12-31	1	
2222	20	0	0	2005-01-01	2015-12-31	1	Mieter Wohnung 2. Etage
3333	30	0	0	2005-01-01	2015-12-31	1	Mieter Wohnung 3. Etage
4444	40	0	0	2005-01-01	2015-12-31	1	Mieter Wohnung 4. Etage
5555	50	0	0	2005-01-01	2015-12-31	1	Mieter, der in Etage 1 und 2 fahren darf.
6666	60	0	0	2005-01-01	2015-12-31	1	Hausmeister darf in alle Etagen fahren.

Tabelle *Time*



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



5.8.5.3. 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 Türmodul das Relais geschaltet wird.
PortOut	Nummer (Byte)	1	Gibt an, welcher Relaisausgang geschaltet wird. Mögliche Angaben: 1 und 2
Elapse	Nummer (int)	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.
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 Auto- matische 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.

5.8.6. Statusmeldungen der Zutrittskontrolle

Anzeige	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.
20	Ausweis korrekt, Zutritt gestattet.
21	Ausweis nicht in der Liste.
22	ActiveGeneral passt nicht.
23	Gültigkeitszeitraum passt nicht.
24	Keinen passenden Raum gefunden.
25	Keinen passenden Zeitbereich gefunden.
26	Warte auf eine Pin-Eingabe.
27	Pin falsch.
28	Bedrohungcode wurde eingegeben.
29	Die PIN ist korrekt, Zutritt gestattet.
30	Die Master-PIN wurde eingegeben, Zutritt gestattet.
31	PIN-Timeout wurde erreicht.
32	Master-Ausweis korrekt, Zutritt gestattet.
33	NUR-PIN-Eingabe ist korrekt, Zutritt gestattet.
34	Online-TP.
35	Online-PIN.
36	Schließung durchgeführt
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.

neu für die EVO-Line V4 Geräte

Statusmeldungen der Zutrittskontrolle

Anzeige	Zugeordnete Statusmeldung
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.
141#	Digitaler Ausgang 15 ist Low (Aus).
142#	Digitaler Ausgang 15 auf HIGH.(An).
143#	Digitaler Ausgang 15 für die Dauer ELAPSE auf HIGH.
144#	Digitaler Ausgang 16 ist Low (Aus).
145#	Digitaler Ausgang 16 auf HIGH.(An).
146#	Digitaler Ausgang 16 für die Dauer ELAPSE auf HIGH.
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

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.			
Anzeige	Zugeordnete Statusmeldung			
	Master (ZK-Box / ZK Master)	GIS	PHG	PHG IO-Box RS485
60	Digi. Eingang1 Master Low	Digitaler Eingang1 Leser Low	Digi.-1 (IO-Box geschlossen)	Digi. Eingang 1 IO-Box Low
61	Digi. Eingang1 Master High	Digitaler Eingang1 Leser High	Digi.-1 (IO-Box offen)	Digi. Eingang 1 IO-Box High
62	Digi. Eingang2 Master Low	Digitaler Eingang2 Leser Low	Digi.-2 (IO-Box geschlossen)	Digi. Eingang 2 IO-Box Low
63	Digi. Eingang2 Master High	Digitaler Eingang2 Leser High	Digi.-2 (IO-Box offen)	Digi. Eingang 2 IO-Box High
64	Digi. Eingang3 Master Low	Digitaler Eingang3 Leser Low	Digi. 3 Sabotageüberwachung -> Kommunikationskanal OK	not used
65	Digi. Eingang3 Master High	Digitaler Eingang3 Leser High	Digi. 3 Sabotageüberwachung -> Kommunikation-unterbrochen	not used
66	Digi. Eingang4 Master Low	Digitaler Eingang 3 wurde unterbrochen	PHG not used	not used
67	Digi. Eingang4 Master High	Digitaler Eingang 3 wurde kurz geschlossen	PHG not used	not used
68	Digi. Eingang5 Master Low	not used	not used	not used
69	Digi. Eingang5 Master High	not used	not used	not used
70	Digi. Eingang6 Master Low	not used	digi. Eingang 1 am Leser Low nicht bei der Voxio-E-Serie	Digi. Eingang 3 IO-Box Low
71	Digi. Eingang6 Master High	not used	digi. Eingang 1 am Leser High nicht bei der Voxio-E-Serie	Digi. Eingang 3 IO-Box High
72		not used	digi. Eingang 2 am Leser Low nicht bei der Voxio-E-Serie	Digit. Eingang 4 IO-Box Low
73		not used	digi. Eingang 2 am Leser High nicht bei der Voxio-E-Serie	Digi. Eingang 4 IO-Box High
74		not used	Sabotagekontakt → Gerätezustand OK	Digi. Eingang 5 Sabotagekontakt → IO-Box Gerätezustand OK digi 5
75		not used	Sabotagekontakt → Gerät manipuliert	Digi. Eingang 6 Sabotagekontakt → IO-Box 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			

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:	Status
Feldfunktion :	Zutritt: Status übernehmen

5.8.7. 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. Piepser

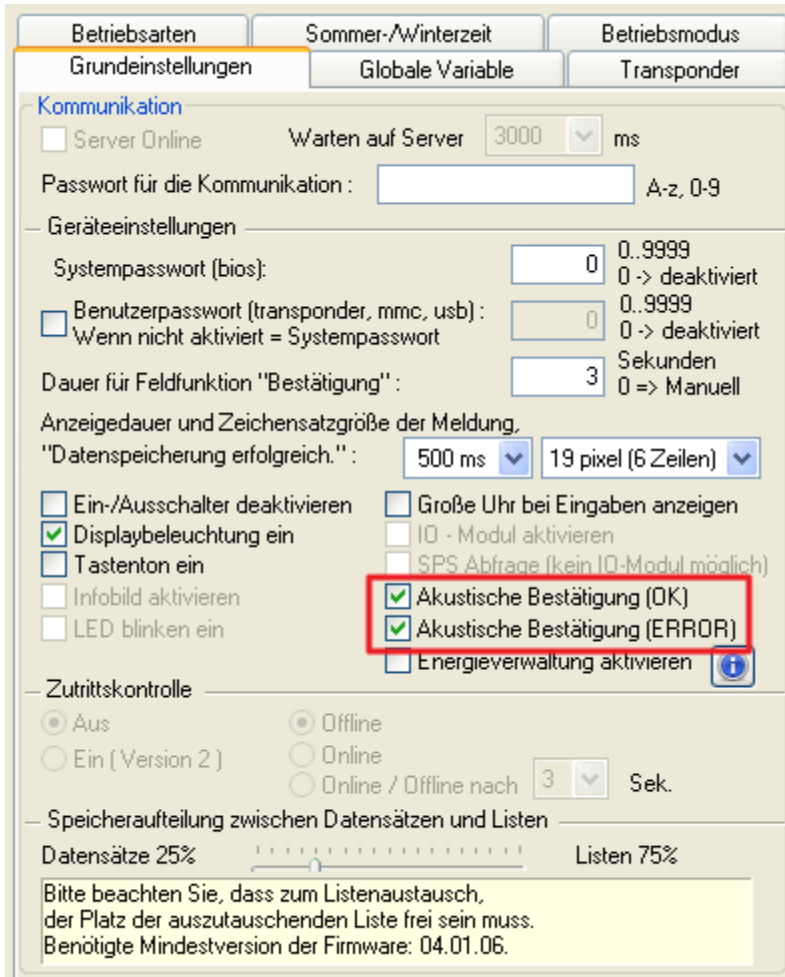
Der Piepser gibt eine Rückmeldung zur Eingabe von Daten.

1 mal Piepsen = Eingabe ist richtig

2 mal Piepsen = Fehler bei der Eingabe

Voraussetzung dafür ist allerdings, dass dieser in den Grundeinstellungen im Setup aktiviert ist.

Siehe Bild.



The screenshot shows the BIOS setup interface for Datafox devices. The 'Kommunikation' (Communication) section is expanded, showing various settings. The 'Akustische Bestätigung (OK)' and 'Akustische Bestätigung (ERROR)' options are checked and highlighted with a red box. Other visible settings include 'Server Online', 'Warten auf Server' (3000 ms), 'Systempasswort (bios)', 'Benutzerpasswort (transponder, mmc, usb)', 'Dauer für Feldfunktion "Bestätigung"', 'Anzeigedauer und Zeichensatzgröße der Meldung', 'Ein-/Ausschalter deaktivieren', 'Displaybeleuchtung ein', 'Tastenton ein', 'Infobild aktivieren', 'LED blinken ein', 'Große Uhr bei Eingaben anzeigen', 'IO - Modul aktivieren', 'SPS Abfrage (kein IO-Modul möglich)', 'Energieverwaltung aktivieren', 'Zutrittskontrolle' (Aus, Offline, Ein (Version 2), Online, Online / Offline nach 3 Sek.), and 'Speicheraufteilung zwischen Datensätzen und Listen' (Datensätze 25%, Listen 75%).

Die Lautstärke der Piezo-Hupe wird über das Menü (Bios) eingestellt.

Siehe dazu das Kapitel Menü (Bios).

6. Technische Daten ZK-MasterIV

ZK-MasterIV HW-Version 2.1 / V3.0

Hardwareversion		V2.1 (Auslieferung bis 2010)	V3.0
System	Uhr	Echtzeituhr	
Daten-Speicher	Flash	2 MB; 100.000 Schreibzyklen	4 MB; 100.000 Schreibzyklen
	Speichererweiterung (optional)	MMC-/SD-Card; max. 1 GB	
Stromversorgung	Netzteil	12 V – 24 V Wechsel- oder Gleichspannung	
	Uhr / RAM Pufferung	Lithiumbatterie	Lithiumbatterie + Goldcap
	Leistungsaufnahme	max. 6 W	
Abmessungen	Länge	205 mm x 120 mm x 40 mm	
Gewicht	ohne Netzteil	400 g	
Umgebungswerte	Umgebungstemperatur	-20 °C bis +70 °C (mit Mobilfunkmodem: MC55: -20 °C bis +55 °C)	
	Schutzart	IP40	
Software	Konfigurationsprogramm	Setupprogramm zum Konfigurieren ohne Programmieraufwand	
	Kommunikationstools	DLL oder C-Source-Code für Einbindung in Anwendung	
Datenübertragung	RS232 / RS485	RS232 im Grundgerät (RS485 optional)	
	TCP/IP (optional)	TCP/IP-Betrieb mit integriertem TCP/IP-Stack	
	WLAN (optional)	wireless LAN module built-in	
	GSM / GPRS (optional)	online per Internet über GSM und GPRS	
	Bluetooth (optional)	Bluetooth Modul integriert; Reichweite bis max. 100 m	
	USB-Schnittstelle (optional)	zur Kommunikation mit einem PC, im Terminal integriert	
	USB-Schnittstelle (optional)	für Datenübertragung per USB-Stick (schließt SD-Card aus)	
Lesegeräteanschluss	RS232 extern	Anschluss von Barcodeleser, Magnetkartenleser etc.	
Zutritt-Optionen	RS485 extern	Anschluss von bis zu 16 externen Türmodulen / Zutrittslesern	
	Türöffner-Relais	2 x 42 V AC oder 30 V DC	2 x max. 60 V, 2 A, 60 W
	Türüberwachung	2 x digitaler Eingang	
Optionen	Transponderleser extern	Anbindung per RS232 / RS485	

Technische Änderungen vorbehalten.

6.1. Technische Daten digitale Eingänge

Parameter	Bez.	Min	Typ	Max	Einheit
Eingangsspannung	V_{In}	0		30	V
Max. Eingangsspg. für low	V_{ILmax}			2	V
Max. Eingangsspg. für high	V_{IHmin}	4,0			V
Eingangsstrom ($V_{In} = 12V$)	I_{In}		6		mA
Eingangsfrequenz	f_{In}			5	kHz

6.2. Technische Daten digitale Ausgänge

Parameter	Bez.	Min	Typ	Max	Einheit
Schaltspannung DC (peak AC)	V_L	0		60	V
Schaltstrom DC (peak AC)	I_L			0,5	A
Schaltstromspitzen ($t=100ms$)	I_{Peak}			1,0	A
Leckstrom	I_{Leak}		1		nA
Ausgangswiderstand	R_{On}		0,83	2,5	Ω
Schaltfrequenz	F_L			100	Hz

7. FAQ

Eine umfangreiche Sammlung von FAQ finden Sie auf unserer Homepage.

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

8. Index

B

Bestimmungsgemäßer Gebrauch und
Umweltschutz 5

D

Deviceinstaller 30
DIP-Schalter ZK 68

E

Einleitung 2
Energie 5
Entsorgung 6

F

FAQ 91
Feiertagssteuerung ZK 68
Firmware 8, 10

G

Gerät 11
GPRS 47

H

HTTP über LAN 24

K

Kommunikation 21
Umschalten 21
Kommunikationsschlüssel 21
Konformitätserklärung 1

M

Modem 44
Montage 16

P

Piepser/Buzzer 90
POE 17

R

RS 232 21
RS 485 23

S

Schleusenfunktion 62

Sicherheit 1

SMS 49

Empfang

Message 50

Service 50

Signalverarbeitung 50

Senden 49

Status 15

GPRS 15

Systemaufbau 7

Systemvoraussetzungen / Hardware 7

T

TCP/IP 24

Comserver 27, 28

UDS 1100 28

Technische Daten ZK-MasterIV 91

Treiberinstallation USB 41

U

USB 41

USB an PC 41

USB-Stick 41

V

Verschlüsselung 21

W

Wartung 50

W-Lan 30

WLAN Grundeinstellung 30

WLANConfig 30

Z

Zeitsteuerung 68

Zu Ihrer Sicherheit 1

Zutritt mit PHG 52