KeTop

KeTop T15xWL / CB4xx
Safe Wireless System (T15xWL / CB4xx)
Projektierungshandbuch V 1.07

Originalbetriebsanleitung

KEBA
Automation by innovation.

Dokument: V 1.07
Seitenanzahl: 280

© KEBA 2021
Änderungen im Sinne der technischen Weiterentwicklung vorbehalten. Angaben erfolgen ohne Gewähr.

Wir wahren unsere Rechte.

KEBA Industrial Automation GmbH
Reindlstraße 51, 4040 Linz, Austria
+43 732 7090-0, +43 732 7309-10, keba@keba.com

Informationen zu KEBA und zu unseren Niederlassungen finden Sie unter www.keba.com.

Änderungsverzeichnis

Version	Datum	Änderung in Kapitel	Beschreibung	Geändert von
1.00	07-2021	-	Neu erstellt	hasl
1.01	10-2021	Diverse Kapitel	Änderung auf neue Firmenstruktur, UKCA, Normen neu strukturiert	hasl
1.02	03-2023	Diverse Kapitel, Gerätekonfiguration, Profinet-Konfiguration, Verbindungsprotokolle, Reinigung des Touchscreens, Robotik-Tastatur, Richtlinien, Normen und Verordnungen	Neue CB4xx Varianten hinzugefügt, Bedienbereichsüberwachung erweitert, diverse Aktualisierungen, neue Tastaturen hinzugefügt, Überarbeitung der Normen	hasl, rmr
1.03	05-2023	Sicherheitshinweise, Bedienbereichsüberwachung, Frontansicht Handbediengeräte, Anzeigen und Bedienelemente, Basisstation CB41x, Basisstation CB42x, Konfiguration, Validierung, Verbinden mit der Basisstation, Sicherheitskennwerte, Zubehör, Konformitätserklärung	Diverse Änderungen und Ergänzungen	rmr
1.04	11-2024	Spannungsversorgung, Montage- und Einbauhinweise, Montage der Basisstation, Basisstation CB42x, Prozessdatenabbild, Ruhezustand konfigurieren, Betrieb und Bedienung, Technische Daten Basisstation, Akku, Normen für den amerikanischen Markt, Konfiguration, Typenschild, Zubehör	Inhalt aus Kapitel gestrichen, Positionierung der Basisstation aktualisiert, Grafiken aktualisiert, Anschlüsse und Verdrahtung angepasst, Daten aktualisiert, Diverse Anpassungen, Betriebszustand hinzugefügt, Einschaltstrom ergänzt, Inhalt und technische Daten erweitert, UL 1740 entfernt, Unterbrechen des AutoLogon hinzugefügt, Basisstation CB43x hinzugefügt, UKCA entfernt, Zusatz-Akku hinzugefügt	ext_klapper
1.05	03-2025	Instandhaltung, Zubehör	Backup mit BSS geändert, Bestellnummern hinzugefügt	ext_klapper
1.06	07-2025	Einleitung, Windows-Einstellungen, Konfiguration	EtherCAT ergänzt, Bestimmungsgemäßer Gebrauch erweitert, ePKEA hinzugefügt, Information über Display-Helligkeit >70 % hinzugefügt	ext_klapper

© KEBA 2021

1.07	04-2026	Anzeigen und Bedienelemente , Zubehör, Diverse Kapitel	CNC-Tastatur hinzugefügt, Tragegurt zu Schutzhülle hinzugefügt, Aktualisierung EU-Batterierichtlinie, BBÜ, Dip-Schaltern, neuem Akku, Displayschutzfolien, Intel Atom x6211, Bestellübersicht und Fehlerzuständen, Typenschild, WEEE- und Entsorgungskennzeichnung sowie Batterieangaben aktualisiert	ext_klapper, bebe

KEBA © KEBA 2021

Inhaltsverzeichnis

1 Einleitung 13
1.1 Zweck des Dokuments 13
1.2 Voraussetzungen 13
1.3 Bestimmungsgemäßer Gebrauch 14
1.3.1 Produkte 15
1.3.2 Cybersicherheit 16
1.3.3 Defense in Depth 40
1.3.4 Geschützte Umgebung 40
1.3.5 Netzwerkarchitektur 42
1.3.6 Netzwerkeigenschaften 47
1.3.7 Fernzugriff 49
1.3.8 Referenz-IACS 50
1.4 Hinweise zu diesem Dokument 52
1.4.1 Inhalt des Dokuments 52
1.4.2 Im Dokument nicht enthalten 53
1.5 Weiterführende Dokumentation 53
1.6 Konformität der sicheren Feldbusse 53
1.6.1 EtherCAT Erklärungen 53
1.6.2 PROFINet / PROFIsafe Erklärungen 54
1.7 Information in Bezug auf MRL 2006/42/EG 54
1.7.1 Quantitative Sicherheitsangaben für Not-Halt und Zustimmeinrichtung 54
1.7.2 Beziehung zwischen Performance Level und Safety Integrity Level 54
1.7.3 Abkürzungen 55
1.8 Not-Halt-Schalter 55

2 Sicherheitshinweise 57
2.1 Darstellung 57
2.2 Allgemeine Sicherheitshinweise 58
2.3 Sicherheitshinweise zur Personensicherheit 60
2.4 ESD-Hinweise 63

3 Systemübersicht 65
3.1 Bedienbereichsüberwachung / BBÜ (optional) 66
3.2 Bestellübersicht 70

4 Beschreibung der Handbediengeräte 73
4.1 Frontansicht 73

© KEBA 2021

4.2 Rückansicht 74
4.3 Handhabung 74
4.4 Typenschild 75
4.4.1 Typenschild Celeron N2807 75
4.4.2 Typenschild Intel Atom x6211 76
4.5 Anzeigen und Bedienelemente 77
4.5.1 Standardtastatur 77
4.5.2 Robotik-Tastatur 78
4.5.3 CNC-Tastatur 80
4.5.4 Status-LEDs 81
4.5.5 "Ident"-Taster 82
4.5.6 Touchscreen 82
4.6 Anschlüsse und Verdrahtung 83
4.6.1 Anschlussschacht 83
4.6.2 Akku anstecken 83
4.6.3 Spannungsversorgung 84
4.6.4 Beleuchteter Not-Halt 84
4.6.5 Zustimmtaster 86
4.6.6 USB-Port 89

5 Basisstation CB41x 91
5.1 Frontansicht 91
5.2 Rückansicht 92
5.3 Unterseite 92
5.4 Oberseite 93
5.5 Typenschild 93
5.6 Anzeigen und Bedienelemente 93
5.6.1 Status-LEDs 94
5.6.2 Verbindungs LEDs 94
5.6.3 Status-LED-Balken 95
5.6.4 "Pairing Reset" Schaltfläche 95
5.7 Montage- und Einbauhinweise 96
5.7.1 Positionierung der Basisstation 96
5.7.2 Bohrschablone für Wandmontage 97
5.7.3 Montage der Basisstation 97
5.8 Anschlüsse und Verdrahtung 99
5.8.1 Klemmleiste S1 / Spannungsversorgung 101
5.8.2 Klemmleiste S2 102
5.8.3 Klemmleiste "Signal" 103
5.8.4 Klemmleiste "Pairing" / "Remote Pairing" Ausgänge 104
5.8.5 Klemmleisten Fast Response Buttons 105
5.8.6 Ethernet 106

KEBA © KEBA 2021

5.8.7 Änderungen an der Verkabelung ... 107
5.8.8 Schließen der Basisstation ... 107
5.8.9 Not-Halt ... 108
5.8.10 Anschlussbeispiel für die Zustimmfunktion mit Überwachungsgerät (PILZ PNOZ s3) ... 109
5.8.11 Anschlussbeispiel für Zustimmfunktion und Not-Halt mit KEBA Sicherheitssteuerung ... 110

6 Basisstation CB42x ... 112
6.1 Frontansicht ... 112
6.2 Rückansicht ... 113
6.3 Unterseite ... 113
6.4 Oberseite ... 114
6.5 Typenschild ... 114
6.6 Anzeigen und Bedienelemente ... 114
6.6.1 Status-LEDs ... 115
6.6.2 Verbindungs LEDs ... 115
6.6.3 Status-LED-Balken ... 116
6.6.4 "Pairing Reset" Schaltfläche ... 116
6.7 Montage- und Einbauhinweise ... 117
6.7.1 Positionierung der Basisstation ... 117
6.7.2 Bohrschablone für Wandmontage ... 118
6.7.3 Montage der Basisstation ... 118
6.8 Anschlüsse und Verdrahtung ... 120
6.8.1 Interne Verkabelung ... 122
6.8.2 Klemmleiste S1 / Spannungsversorgung ... 122
6.8.3 Klemmleiste S2 ... 123
6.8.4 Klemmleiste "Signal" ... 124
6.8.5 Ethernet ... 125
6.8.6 PROFINET ... 125
6.8.7 Änderungen an der Verkabelung ... 126
6.8.8 Schließen der Basisstation ... 126
6.8.9 Not-Halt ... 127
6.9 Fehlerquittierung ... 128

7 Basisstation CB43x ... 129
7.1 Frontansicht ... 129
7.2 Rückansicht ... 130
7.3 Unterseite ... 130
7.4 Oberseite ... 131
7.5 Typenschild ... 131
7.6 Anzeigen und Bedienelemente ... 131
7.6.1 Status-LEDs ... 132

© KEBA 2021

7.6.2 Verbindungs LEDs 132
7.6.3 Status-LED-Balken 133
7.6.4 "Pairing Reset" Schaltfläche 134
7.7 Montage- und Einbauhinweise 134
7.7.1 Positionierung der Basisstation 134
7.7.2 Bohrschablone für Wandmontage 135
7.7.3 Montage der Basisstation 136
7.8 Anschlüsse und Verdrahtung 137
7.8.1 Interne Verkabelung 140
7.8.2 Klemmleiste S1 / Spannungsversorgung 140
7.8.3 Klemmleiste S2 141
7.8.4 Klemmleiste "Signal" 141
7.8.5 Ethernet 142
7.8.6 EtherCAT 143
7.8.7 Änderungen an der Verkabelung 144
7.8.8 Schließen der Basisstation 144
7.8.9 Not-Halt 145
7.9 Fehlerquittierung 145

8 Konfiguration 147
8.1 Box-ID Konfiguration 147
8.2 F-Adressierung (nur bei CB42x und CB43x) 148
8.3 Bedienbereichs-Konfiguration (sicherheitsrelevant) 149
8.4 Gerätekonfiguration (Device Config) 150
8.4.1 Basestation 151
8.4.2 Diagnosis data 156
8.4.3 Display 156
8.4.4 Licenses 157
8.4.5 Network 157
8.4.6 Reboot 164
8.4.7 Shutdown 164
8.4.8 Version info 164
8.5 PROFINET-Konfiguration (nur bei CB42x) 165
8.5.1 Prozessdatenabbild 165
8.6 EtherCAT / FSoE-Konfiguration (nur bei CB43x) 168
8.6.1 Prozessdatenabbild 168
8.7 Ruhezustand konfigurieren 170
8.8 Fernzugriff auf das KeTop 171
8.8.1 Fernzugriff über OpenSSH 172
8.9 Security-Einstellungen 173
8.9.1 (De-) Installation 174
8.9.2 Whitelisting über AppLocker 175

KEBA © KEBA 2021

8.9.3 Kiosk Desktop ... 175
8.9.4 KEBA Write Filter ... 180
8.10 Verbindungsprotokolle ... 181
8.11 Tastenmanagement ... 183
8.11.1 Tastencodes ... 184
8.12 Windows Einstellungen ... 186
8.13 Programmierung ... 188

9 Betrieb und Bedienung ... 189
9.1 Hochlauf ... 189
9.2 Ausschalten des KeTops ... 190
9.3 Betriebszustände Basisstation ... 190
9.4 Betriebsverhalten ... 191
9.5 Ladeverhalten des Akkus ... 192
9.6 "System State" Anzeige ... 193

10 Validierung ... 194
10.1 Validierung der Abstandsmessung ... 194

11 Verbinden mit Basisstation ... 195

12 Diagnose ... 201

13 Instandhaltung ... 203
13.1 Reinigung des Touchscreens ... 203
13.2 Wechseln des Akkus ... 204
13.3 Erstellen eines Service Mediums ... 204
13.4 Erstellen eines Backups ... 205
13.5 Wiederherstellen eines Backups / Durchführen eines Updates ... 208
13.6 Wechseln der Speicherkarte ... 212

14 Entsorgung ... 214
14.1 Entsorgung der Baugruppe ... 214
14.2 Entsorgung des Akkus ... 214

15 Technische Daten ... 217
15.1 Allgemein ... 217
15.2 Umgebungsbedingungen ... 217
15.3 Sicherheitskennwerte ... 217
15.3.1 Systemreaktionszeit mit sicherer Feldbusanbindung (bei CB42x und CB43x) ... 219
15.4 Mechanische Eigenschaften ... 220
15.5 Batterie / Akku ... 220

© KEBA 2021

15.6 Technische Daten Handbediengerät ... 221
15.6.1 Allgemein ... 221
15.6.2 Versorgung ... 221
15.6.3 Rechnerkern ... 221
15.6.4 Schnittstellen ... 222
15.6.5 Abmessungen, Gewicht ... 223
15.7 Technische Daten Basisstation ... 223
15.7.1 Versorgung ... 223
15.7.2 Schnittstellen ... 223
15.7.3 Klemmleisten ... 224
15.7.4 Zustimmfunktion ... 225
15.7.5 Not-Halt-Funktion ... 226
15.7.6 Abmessungen, Gewicht ... 226

16 Optionale Bedienelemente ... 228
16.1 Drehschalter mit 16 Positionen ... 228
16.2 Schlüsselschalter ... 228
16.3 Leuchtdrucktaster ... 228
16.4 Handrad ... 229
16.5 Digitaler Joystick ... 229
16.6 Kamera ... 230

17 Zubehör ... 231
17.1 KeTop CS 15x Ladestation ... 231
17.2 Netzteil ... 233
17.3 Akku ... 233
17.3.1 Akku Celeron N2807 ... 234
17.3.2 Akku Atom x6211 ... 235
17.4 Schutzhülle / Trageset ... 236
17.4.1 Anbringen der Schutzhülle ... 238
17.4.2 Reinigung ... 240
17.4.3 Lagerung und Transport ... 240
17.5 Griff und Handschlaufe ... 240
17.5.1 Montage ... 241
17.6 Zusatz-Akku ... 243
17.6.1 Zusatz-Akku verwenden ... 246
17.6.2 Zusatz-Akku laden ... 246
17.6.3 Technische Daten ... 247
17.7 Rückwand für rückseitige Kabelmontage (nur für CB41x) ... 249
17.8 Displayschutzglas ... 249

18 Richtlinien, Normen und Verordnungen ... 251
18.1 EU-Richtlinien / Verordnungen ... 251

KEBA © KEBA 2021

18.2 Normen zur Überprüfung der Konformität ... 251
18.3 Sonstige Normen ... 252
18.4 Verordnungen ... 255
18.5 Normen für den amerikanischen Markt ... 255
18.6 Normen für den kanadischen Markt ... 256
18.7 Normen für den japanischen Markt ... 257

19 EU-Konformitätserklärung ... 261

20 Anhang: Inbetriebnahme ... 264

21 Anhang: Sicherheit von Maschinen ... 265
21.1 Risikobeurteilung ... 266
21.2 Grundsätze für die Integration des KeTops ... 266
21.3 Technische Unterlagen ... 267
21.4 Stand der Technik ... 268
21.5 Konformitätsvermutung mit harmonisierten Normen ... 268
21.6 Auswahl von Performance Level und Kategorie nach EN ISO 13849-1 ... 268
21.7 Anwendung von Handbediengeräten in Sonderbetriebsarten ... 270
21.8 Hinweise zum Schalter für das Stillsetzen im Notfall ("Not-Halt") ... 270
21.9 Bedienelemente zum Stillsetzen im Notfall ... 271
21.10 Hinweise zum Zustimmtaster ... 272

22 Anhang: Chemikalienbeständigkeit ... 275

23 Anhang: Begriffe und Definitionen ... 277

Index ... 278

© KEBA 2021

KEBA © KEBA 2021

1 Einleitung

1.1 Zweck des Dokuments

Dieses Dokument beschreibt das Safe Wireless System. Dieses besteht aus einem akkubetriebenen mobilen Handbediengerät und einer fest installierten Basisstation. Das Handbediengerät verfügt über die Sicherheitsfunktion "Not-Halt" und einen Zustimmtaster, welche kabellos ("wireless") mit der Basisstation verbunden sind.

In diesem Dokument sind alle relevanten Anforderungen aus der MRL 2006/42/EG enthalten (Beschreibung der Maschine siehe Kapitel 3 - 5).

Information

Dieses Handbuch richtet sich ausschließlich an die in diesem Handbuch aufgelisteten Zielgruppen. Die für Endkunden notwendigen Sicherheitshinweise müssen vom Maschinenbauer oder Systemanbieter in die Betriebsanleitung für Endkunden in der jeweiligen Landessprache übernommen werden!

1.2 Voraussetzungen

Dieses Dokument enthält Informationen für Personen mit den folgenden Voraussetzungen:

Zielgruppe	Voraussetzung an Wissen und Können
Sicherheitsingenieur für "Funktionale Sicherheit"	Technische Grundausbildung (Fachhochschule, Ingenieur-Ausbildung oder entsprechende Berufserfahrung), Kenntnisse über: ● die Grundlagen der funktionalen Sicherheit, ● alle einschlägigen Normen und Sicherheitsvorschriften der Maschine/Anlage, insbesondere auch Kenntnisse über Validierung nach EN ISO 13849-2, ● spezielle Gefahrenpotentiale der Maschine/Anlage und des Produktionsprozesses, ● konkrete Schutzmaßnahmen zur Vermeidung der maschinenspezifischen Gefährdungen (aus Gefahren- und Risikoanalyse), ● Funktionsweise und Anwendungsgrenzen der Sicherheitsbauteile (einschließlich Sicherheits-SPS), ● vertiefte Kenntnisse der nationalen Unfallverhütungsvorschriften.
Projektierer	Technische Grundausbildung (Fachhochschule, Ingenieur-Ausbildung oder entsprechende Berufserfahrung). Kenntnisse über: ● aktuell gültige Sicherheitsvorschriften, ● die Arbeitsweise einer SPS, ● die Applikation.

© KEBA 2021

Zielgruppe	Voraussetzung an Wissen und Können
Elektromonteur	Elektrotechnische Fachausbildung (nach branchenüblichen Ausbildungsrichtlinien). Kenntnisse über: ● aktuell gültige Sicherheitsvorschriften, ● Verdrahtungsrichtlinien, ● Schaltpläne, ● fachgerechtes Herstellen elektrischer Anschlüsse nach nationalen und internationalen Vorschriften.
Inbetriebnehmer	Technische Grundausbildung (Fachhochschule, Ingenieur-Ausbildung oder entsprechende Berufserfahrung). Kenntnisse über: ● aktuell gültige Sicherheitsvorschriften, ● die Arbeitsweise der Maschine oder Anlage, ● grundlegende Funktionen der Applikation, ● Systemanalyse und Fehlerbehebung, ● die Einstellmöglichkeiten an den Bedienvorrichtungen.
Servicetechniker	Technische Grundausbildung (Fachhochschule, Ingenieur-Ausbildung oder entsprechende Berufserfahrung). Kenntnisse über: ● die Arbeitsweise einer SPS, ● aktuell gültige Sicherheitsvorschriften, ● die Arbeitsweise der Maschine oder Anlage, ● Diagnosemöglichkeiten, ● systematische Fehleranalyse und -behebung.

1.3 Bestimmungsgemäßer Gebrauch

Der bestimmungsgemäße Gebrauch der Handbediengeräte erstreckt sich von der Beobachtung und Parametrierung bis hin zur Bedienung von Maschinen, wie zum Beispiel:

- Spritzgießmaschinen
- Roboter
- Textilmaschinen
- Druckereimaschinen

in den Normalbetriebsarten, wie beispielsweise

- Automatik

sowie in halbautomatischen oder manuellen Sonderbetriebsarten, wie beispielsweise

- Einrichten
- Teachen
- Testlauf

KEBA © KEBA 2021

Als Sicherheitsfunktionen stehen ein Zustimmtaster, sowie ein beleuchteter Not-Halt zur Verfügung.

Not-Halt und Zustimmtaster sind zweikreisig ausgeführt und ermöglichen eine Umsetzung der Kategorie 4 PL e nach EN ISO 13849-1 unter Berücksichtigung der Betätigungszyklen im Hinblick auf die B_{10D} Werte der Sicherheitsbauteile.

Die Auswahl des für die Maschine geeigneten Handterminals sowie die Projektierung der möglichen Zusatzoptionen muss ausgehend von der gesetzlich erforderlichen Gefahren- und Risikobeurteilung im Verantwortungsbereich des Maschinenherstellers erfolgen.

Beachten Sie bitte in Bezug auf den bestimmungsgemäßen Gebrauch des Handterminals auch die Anhänge.

KEBA-Produkte wie KeTop, KeControl, KeConnect und KeDrive sind Komponenten für industrielle Automatisierungs- und Steuerungssysteme ("industrial automation and control system", IACS). Ein IACS kann für den Betrieb einer Vielzahl von Anlagen verwendet werden. Es kann zur Steuerung einzelner Maschinen (wie z.B. Spritzgießmaschinen), aber auch zum Betrieb größere Systeme (wie z.B. ganzer Anlagen) verwendet werden.

KEBA-Produkte können für jede Art von Maschine oder Anlage verwendet werden, wenn das Produkt die notwendigen Anforderungen erfüllt und dem bestimmungsgemäßen Gebrauch des Produktes entspricht. Sie sind als IACS-Komponenten mit dem Fokus auf Maschinenbauer konzipiert und können auch in der Fabriksautomation eingesetzt werden, die mehrere Maschinen steuern.

1.3.1 Produkte

Die KEBA-Produkte für IACS sind in folgende Produktfamilien eingeteilt:

- KeTop
  - Handbediengeräte
  - Stationäre Bediengeräte
- KeControl
  - Steuerungen
  - Industrie PCs
  - Robotersteuerungen
- KeConnect
  - Digitaler Eingang/Ausgang
  - Analoger Eingang/Ausgang
  - Temperatureingang
  - PWM-Ausgang
  - Geber-Schnittstellen
  - RS232-, RS422- und RS485-Schnittstellen
  - IO-Link-Schnittstellen
  - …
- KeDrive
  - Servoregler

© KEBA 2021

- KeStudio
  - Software-Werkzeuge für KeTop-, KeControl-, KeConnect- und KeDrive-Geräte

Jede Produktfamilie enthält eine breite Palette von Produkten. Sie enthalten physische Produkte wie ein Steuerungs-Gerät oder ein digitales Ausgabegerät. Sie enthalten auch Software, die für den Betrieb dieser Geräte erforderlich ist. Bei dieser Software kann es sich sowohl um Software handeln, die auf den Geräten läuft, als auch um Software, die zur Kommunikation mit den Geräten verwendet wird.

1.3.2 Cybersicherheit

KEBA-IACS-Komponenten folgen einem gemeinsamen Satz von Sicherheitsgrundsätzen. Diese Sicherheitsgrundsätze ermöglichen es dem Eigentümer der Anlage, ein hohes Sicherheitsniveau zu erreichen. Sie ermöglichen auch ein Verständnis dafür, wie Sicherheit konzipiert ist und wie sie in der Praxis funktioniert. Zunächst werden die allgemeinen Sicherheitsprinzipien für alle KEBA-IACS-Komponenten vorgestellt. Danach werden die spezifischen Sicherheitsprinzipien von Geräten für Automatisations-Netzwerke und von Geräten für Maschinen-Netzwerke beschrieben. In den verbleibenden Kapiteln liegt der Schwerpunkt auf der Sicherheit von Softwarediensten und Funktionen von KEBA-IACS-Komponenten.

Der Eigentümer der Anlage legt das erforderliche Sicherheitsniveau fest. Wenn die erforderliche Sicherheitsstufe niedrig ist, können bestimmte Sicherheitsprinzipien weggelassen werden. Daher entscheidet der Anlagenbesitzer, welche Sicherheitsprinzipien tatsächlich ausgeführt werden und vorhanden sind. Die Konfiguration der KEBA-IACS-Komponenten erlaubt es, Sicherheitsmerkmale zu deaktivieren.

Jede KEBA-IACS-Komponente hat individuelle Funktionalitäten, um die Anforderungen von Maschinenbauern und Systemintegratoren zu erfüllen. Die Liste der von KEBA-IACS-Komponenten unterstützten Software-Dienste und -Funktionen hängt daher vom jeweiligen Produkt ab. Die tatsächlich unterstützten Software-Dienste und Features sind in der produktspezifischen Dokumentation dokumentiert. Dieses Dokument verweist auf Produktfamilien, um einen Überblick über die unterstützten Softwaredienste und -funktionen zu geben.

Information

Nicht alle KEBA-Geräte mit Windows als Betriebssystem unterstützen die Features in genau der gleichen Weise, aber die Prinzipien sind genauso gültig und müssen teilweise mit Windows-Standardfunktionen umgesetzt werden (z.B. Benutzerverwaltung, …).

1.3.2.1 Ziele der Cybersicherheit

Die Cybersicherheit konzentriert sich auf folgende Ziele, die für IACS in folgender Reihenfolge gelten:

1) Verfügbarkeit
2) Integrität

KEBA © KEBA 2021

3) Vertraulichkeit

Die Verfügbarkeit hat in der Regel die höchste Priorität, da ein Produktionsstopp zu erheblichen finanziellen Verlusten führen kann. An zweiter Stelle steht häufig die Integrität, da die kontrollierten Prozesse und Maschinen nur innerhalb bekannter Grenzen bestimmungsgemäß betrieben werden dürfen, um die Qualitätsanforderungen zu erfüllen. IACS verwenden oder schützen keine Geschäftsgeheimnisse wie Finanzdaten. Anders als bei IT-Systemen ist bei IACS die Vertraulichkeit daher in der Regel weniger wichtig als die Verfügbarkeit und Integrität.

1.3.2.2 Allgemeine Sicherheitsgrundsätze

Die folgenden allgemeinen Sicherheitsgrundsätze gelten für alle KEBA-IACS-Komponenten.

Authentifizierung

Die Authentifizierung ist eine Voraussetzung für jeden Zugriff auf eine IACS-Komponente. Unabhängig davon, ob Informationen gelesen oder Aktionen ausgeführt werden sollen, ist zunächst eine erfolgreiche Authentifizierung erforderlich. Es gibt mehrere Mechanismen, die eine sichere Authentifizierung ermöglichen:

- **Passwort**: Passwörter werden immer noch zur Authentifizierung verwendet. Wenn Passwörter verwendet werden, dann sollte darauf geachtet werden, dass die Passwörter ein ausreichendes Sicherheitsniveau gegen Bedrohungen wie Wörterbuchangriffe oder Brute-Force-Angriffe bieten. Passwörter werden z.B. von der Weboberfläche und DevAdmin verwendet.
- **Schlüssel**: Asymmetrische kryptografische Schlüssel sind der Stand der Technik für die Authentifizierung. Solche Schlüssel werden z.B. von SSH verwendet.
- **Zertifikat**: Zertifikate sind öffentliche Schlüssel, die von einer Zertifizierungsstelle (CA) unterzeichnet werden. Zur Authentifizierung wird der Besitz des privaten Schlüssels angezweifelt und die Unterschrift der CA validiert. Zertifikate werden z.B. von DevAdmin, OPC UA und OpenVPN verwendet.
- **Geografischer Standort**: Der Standort kann für die Authentifizierung verwendet werden, wenn für diesen Ort physische Zugangsbeschränkungen bestehen. Dies ist der Fall bei Geschäftsräumen, die nur mit einer gültigen Schlüsselkarte betreten werden können, oder bei einem Schrank, der nur mit einem eindeutigen Schlüssel geöffnet werden kann. Darüber hinaus kann ein Gerät, das für die Bereitstellung von Funktionen für physisch anwesende Personen konzipiert ist, auch den Standort zur Authentifizierung verwenden. Der geografische Standort wird z.B. von Anzeige- und Bedienelementen der Geräte KeControl, KeTop und KeDrive zur Authentifizierung verwendet.

© KEBA 2021

- **Schlüsselkarte**:Schlüsselkarten sind ein weit verbreiteter Mechanismus zur Authentifizierung. Auf der Schlüsselkarte ist ein Geheimnis gespeichert. Dieses Geheimnis wird für die Authentifizierung verwendet. Schlüsselkarten werden z.B. bei der Visualisierung auf KeTop-Geräten verwendet.

Die zur Authentifizierung verwendeten Geheimnisse müssen stark genug sein, um die vom Eigentümer der Anlage geforderte Sicherheitsstufe zu erfüllen. Sie dürfen nicht erraten werden können. Mit Hilfe von Richtlinien kann sichergestellt werden, dass Passwörter und Schlüssel stark genug sind und nicht veröffentlicht werden können. Die Verwaltung der Authentifizierung erfolgt über spezielle Schnittstellen und Tools. Für KEBA-Geräte sind KeStudio und "DevAdmin" für die Benutzer- und Authentifizierungsverwaltung verfügbar.

Keine Standardpasswörter

Standardpasswörter sind ein gängiger Angriffsvektor. Selbst ein starkes Standardpasswort erhöht die Sicherheit nicht, da jedes Standardpasswort einer breiten Gruppe von Personen bekannt ist. Das Gleiche gilt für private Standardschlüssel. Daher bieten KEBA-IACS-Komponenten keine Standardpasswörter oder private Schlüssel. Alle Passwörter und die entsprechenden öffentlichen Schlüssel der privaten Schlüssel müssen bei der Einrichtung oder später gesetzt werden. Wenn kein Passwort oder öffentlicher Schlüssel gesetzt ist, ist eine Authentifizierung für den entsprechenden Dienst nicht möglich und der Dienst kann nicht verwendet werden..

Verschlüsselung

Nach erfolgreicher Authentifizierung können die Daten übertragen werden. Diese Daten sind dem Risiko des Abhörens und der Manipulation ausgesetzt. Daher wird eine Verschlüsselung verwendet, um die Vertraulichkeit und Integrität der übertragenen Daten zu gewährleisten. Die verwendeten Protokolle müssen modernste Verschlüsselungsalgorithmen unterstützen. Verschlüsselte Kommunikation wird von Protokollen wie z. B. HTTPS, SSH, OPC UA und OpenVPN bereitgestellt.

Geringste Berechtigung

Eine erfolgreiche Authentifizierung muss den Zugang zu einer minimalen Anzahl von Informationen und Aktionen ermöglichen. Die Einschränkungen können durch den Dienst, auf den zugegriffen wird, und/oder durch den Benutzer, der sich authentifiziert, festgelegt werden. Dieses Prinzip der geringsten Berechtigung senkt das Risiko schwerwiegender Sicherheitslücken, da die Angriffsfläche erheblich reduziert wird. Außerdem begrenzt es die Erlangung von Zugriffsrechten, wenn ein Angreifer die Authentifizierung überwunden hat. Dies bietet insbesondere dann Sicherheitsvorteile, wenn während des Betriebs nur ein Minimum an Berechtigungen genutzt wird und verfügbar ist.

KEBA © KEBA 2021

Beschränkungen auf Basis des authentifizierten Benutzers sind z.B. für Visualisierungen und SSH möglich. Für Visualisierungen können Funktionen und Masken auf bestimmte Benutzer beschränkt werden. Für SSH kann der Shell- und Dateizugriff benutzerbasiert eingeschränkt werden.

Beispiele für dienstbedingte Einschränkungen sind OpenVPN und Displays mit Bedienelementen. Alle bieten einen definierten Satz von Informationen und Aktionen, die zu einer sicheren Nutzung während des Betriebs passen.

Physische Zugangsbeschränkung

Ein IACS kann nicht sicher betrieben werden, wenn der physische Zugang für jedermann möglich ist. Bei physischem Zugriff können z.B. Kabel manipuliert oder vertauscht werden. Dadurch werden die Sicherheitsziele Verfügbarkeit und Integrität verletzt, ohne dass eine digitale Interaktion stattfindet. Daher ist es eine Voraussetzung, dass KEBA-IACS-Komponenten durch eine physische Zugangskontrolle geschützt sind. Zugangsbeschränkungen sind sowohl für die Produktionsräume als auch für den Schrank notwendig. Normalerweise ist der Zugang zum Schrank einer kleineren Gruppe erlaubt als der Zugang zu den Produktionsräumen. Der Zugriff auf die Produktionsräume schließt also nicht automatisch den Zugriff auf den Schrank ein.

Die physische Zugangskontrolle kann mit einfachen Maßnahmen wie Schlüsseln oder Schlüsselkarten eingerichtet werden. Dies ist in der Regel für Mitarbeiter ausreichend. Für externe Gäste oder Techniker sind auch aufwändigere Maßnahmen wie Sicherheitsschleusen mit eigenem Wachpersonal möglich.

1.3.2.3 Geräte im Automationsnetzwerk

Die KEBA-Produktfamilien KeControl und KeTop sind für den Einsatz in Automatisations-Netzwerken konzipiert. Diese IACS-Komponenten sind in der Lage, die oben angeführten allgemeinen Sicherheitsgrundsätze zu erfüllen. Voraussetzung dafür ist, dass die integrierte Firewall dieser Geräte so konfiguriert ist, dass nur sichere Dienste zugelassen werden. Die folgenden sicheren Dienste sind im Einsatz:

- HTTPS (Web-Interface)
- OPC UA
- SSH
- OpenVPN

Je nach den Anforderungen des Anlagenbesitzers kann die Firewall so konfiguriert werden, dass sie alle aktiven Dienste zulässt, unabhängig davon, ob sie sicher sind oder nicht. Dadurch wird natürlich das Sicherheitsniveau des Automatisations-Netzwerkes verringert. Eine weitere Bedrohungs- und Risikobewertung durch den Anlagenbetreiber ist erforderlich, um sicherzustellen, dass auch bei diesen Diensten ohne Authentifizierung und Verschlüsselung das erforderliche Sicherheitsniveau erreicht wird.

KeControl- und KeTop-Geräte können auch als "Boundary protection devices" zwischen dem Automatisations-Netzwerk und dem Maschinen-Netzwerk eingesetzt werden. Die Firewall dieser Geräte behandelt den Datenverkehr netzwerkspezifisch. Der Verkehr aus dem Automatisations-Netzwerk

© KEBA 2021

wird eingeschränkt und kann nur auf ausgewählte Dienste zugreifen; z.B. auf sichere Dienste wie HTTPS. Auf der anderen Seite ist der Verkehr aus dem Maschinen-Netzwerk nicht eingeschränkt und kann auf alle Dienste zugreifen. Außerdem ist das Routing zwischen den beiden Netzen deaktiviert. Auf diese Weise sorgen diese "Boundary protection devices" für eine Segmentierung des Automatisations-Netzwerkes und des Maschinen-Netzwerkes.

KeControl-Produktfamilie

Die Produkte der KeControl-Familie sind Geräte, die in der Lage sind, Kundenapplikationen zur Steuerung von Maschinen und Prozessen auszuführen. Sie sind mit leistungsstarken CPUs ausgestattet und laufen mit Linux als Betriebssystem. Die KEBA-Software ist auf diesen Geräten installiert und ermöglicht es Kunden , Anwendungen mit einer Vielzahl von physikalischen und logischen Schnittstellen zu schreiben. Die installierte KEBA-Software und die Kundenanwendung bestimmen, ob das Produkt als Steuerung, Robotersteuerung oder nur als IPC eingesetzt wird.

KeTop-Produktfamilie

Produkte der KeTop-Familie sind Geräte, die Benutzerschnittstellen wie Displays und Bedienelemente bereitstellen, um die Interaktion von Menschen mit Maschinen und Systemen zu ermöglichen. Die KeTop-Produktfamilie hat verschiedene Unterfamilien mit deutlichen Unterschieden in Bezug auf die Sicherheit:

- **Aktive Bediengeräte**: Sie bieten ein Display mit Touch und zusätzlichen Bedienelementen und sind zusätzlich mit leistungsfähigen CPUs ausgestattet, auf denen ein Betriebssystem läuft. Die GUI-Anwendung läuft direkt auf der CPU des aktiven Bediengerätes. Ein aktives Bediengerät kann als Automatisations-Netzwerkgerät und "Boundary protection device" eingesetzt werden. Das Betriebssystem ist Linux oder Windows.
- **Passive Bediengeräte**: Sie dienen als Monitor und stellen ein Display mit Touch und zusätzlichen Bedienelementen zur Verfügung. Die GUI-Applikation läuft auf einem separaten KeControl-Gerät und das passive Bediengerät wird an dieses Gerät angeschlossen. Ein passives Bediengerät kann nicht als Automatisations-Netzwerkgerät verwendet werden, da es keine Netzwerkschnittstellen hat und nur ein Zubehör für KeControl-Geräte ist.

1.3.2.4 Geräte im Maschinennetzwerk

Die KEBA-Produktfamilien KeConnect und KeDrive sind ausschließlich für den Einsatz als Maschinen-Netzwerkgeräte konzipiert. Maschinen-Netzwerkgeräte sind nicht in der Lage, die allgemeinen Sicherheitsgrundsätze von oben vollständig zu erfüllen. Für die Feldbuskommunikation sind Authentifizierung und Verschlüsselung meist nicht verfügbar. Somit sind der physikalische Zugriffsschutz und das Geringste-Privilegien-Prinzip die einzigen Sicherheitsprinzipien, die für Maschinen-Netzwerkgeräte gefordert werden können. KeConnect- und KeDrive-Geräte erfüllen beide Sicherheitsprinzipi-

KEBA © KEBA 2021

en. KeControl- und KeTop-Geräte erfüllen diese Sicherheitsprinzipien ebenfalls, können aber auch als Automatisations-Netzwerkgeräte eingesetzt werden.

Der physische Zugriffsschutz auf den Schrank, der das Maschinen-Netzwerk enthält, ermöglicht die geografische Lokalisierung als Authentifizierung für alle Maschinen-Netzwerkgeräte. Ein Techniker, der den Schrank öffnen kann, ist berechtigt, die gesamte Software und Hardware des Schranks zu manipulieren. Sowohl die Software als auch die Hardware folgen dem Prinzip der geringsten Privilegien, um den Zugriff auf eine bestimmte Anzahl von Informationen und Handlungen zu ermöglichen.

Die folgenden sicheren Dienste werden für KEBA-Maschinen-Netzwerkgeräte verwendet:

- HTTPS (Web-Interface)
- OPC UA
- SSH (einschließlich SFTP)

Zusätzlich zu den sicheren Diensten sind folgende Dienste und Protokolle ohne Authentifizierung und Verschlüsselung für KEBA-Maschinen-Netzwerkgeräte im Einsatz:

- Feldbusse (EtherCAT, PROFINET, CANopen, EtherNet/IP, …)
- RPC-basierte Dienste
- KVC
- EtherCAT-Mailbox-Gateway
- Steuerungs-Protokolle für nicht-KEBA-Steuerungen (ADS, S7, Modbus)

KeConnect-Produktfamilie

Die Produkte der KeConnect-Familie sind Geräte mit verschiedenen Arten von Eingängen, Ausgängen und Schnittstellen für die Automatisierung von Maschinen und Prozessen. Sie können direkt an die Steuerung angeschlossen werden oder für den dezentralen Einsatz über einen Feldbus mit der Steuerung verbunden werden. KeConnect-Geräte überschreiten keine Grenzen zu anderen sicherheitsrelevanten Zonen. Alle Eingänge, Ausgänge, Schnittstellen und die Kommunikation mit der Steuerung sind auf die Maschine und das Maschinen-Netzwerk beschränkt. Selbst digitale Schnittstellen für Drehgeber oder IO-Link sind nur für die lokale Kommunikation ausgelegt. Die Maschine und das Maschinen-Netzwerk bilden somit eine geschützte Umgebung für den Betrieb von KeConnect-Geräten.

Die neuesten KeConnect-Geräte nutzen als Kommunikationsschnittstelle den Feldbus EtherCAT. Dieser Feldbus verbindet hohe Performance mit geringem Implementierungsaufwand für die Geräte. Die Sicherheit in Form von Authentifizierung und Verschlüsselung steht bei diesem und allen anderen Feldbussen nicht im Vordergrund. Die Sicherheit beruht auf der örtlichen Gegebenheit der Geräte und der physischen Zugangskontrolle. Dies ermöglicht eine wirtschaftliche Umsetzung von Automatisierungslösungen mit hoher Performance.

© KEBA 2021

KeDrive-Produktfamilie

Die Produkte der KeDrive-Familie sind Geräte mit unterschiedlichen Schnittstellen zur Steuerung von Motoren für die Automatisierung von Maschinen und Prozessen. Sie werden in der Regel über einen Feldbus an die Steuerung angeschlossen. Einige Varianten können auch direkt an die Steuerung angeschlossen werden. KeDrive-Geräte überschreiten keine Grenzen zu anderen sicherheitsrelevanten Zonen. Alle Eingänge, Ausgänge, Schnittstellen und die Kommunikation mit der Steuerung sind auf die Maschine und das Maschinen-Netzwerk beschränkt. Selbst digitale Schnittstellen für Geber sind nur für die lokale Kommunikation ausgelegt. Die Maschine und das Maschinen-Netzwerk bilden somit eine geschützte Umgebung für den Betrieb von KeDrive-Geräten.

KeDrive-Geräte verwenden Feldbusse als Kommunikationsschnittstelle. Diese Feldbusse verbinden hohe Performance mit geringem Implementierungsaufwand für die Geräte. Die Sicherheit in Form von Authentifizierung und Verschlüsselung steht bei den Feldbussen nicht im Vordergrund. Die Sicherheit beruht auf der örtlichen Gegebenheit der Geräte und der physikalischen Zugangskontrolle. Dies ermöglicht eine wirtschaftliche Umsetzung von Automatisierungslösungen mit hoher Performance.

Das Software-Tool DriveManager wird zur Konfiguration und Diagnose von KeDrive-Produkten verwendet. Das Tool kommuniziert mit dem Gerät über ein IP-basiertes Protokoll. Das verwendete Kommunikationsprotokoll unterstützt keine Authentifizierung oder Verschlüsselung. Daher ist diese Kommunikation auf das Maschinen-Netzwerk zu beschränken. Von der direkten Nutzung der DriveManager-Kommunikation innerhalb des Automatisations-Netzwerks oder eines anderen Netzwerks ohne zusätzliche Sicherheitsmaßnahmen wird dringend abgeraten. Sichere Tunnel wie OpenVPN können verwendet werden, um dem DriveManager einen sicheren Zugang zu anderen Netzwerken als dem Maschinen-Netzwerk zu ermöglichen.

KeDrive-Geräte unterstützen Passwörter, um den Zugriff auf bestimmte Parameter zu beschränken. Diese Passwörter werden nur verwendet, um verschiedene Filter für die Liste der verfügbaren Parameter bereitzustellen. Der Zugriff auf die Parameter selbst ist durch diese Passwörter nicht geschützt. Die Passwörter von KeDrive-Geräten sind also keine sicherheitsrelevante Funktionalität. Die Sicherheit der KeDrive-Geräte beruht nicht auf diesen Passwörtern.

1.3.2.5 Verwaltung der Authentifizierung

Die Authentifizierung ist die Grundlage für die meisten sicheren Dienste. Die Kommunikationspartner authentifizieren sich gegenseitig auf sichere Art und Weise, bevor die eigentliche verschlüsselte Kommunikation beginnt. Auch der lokale Zugang zu privilegierten Aktionen und Informationen wird durch Authentifizierung geschützt.

Bei der Authentifizierung ist der Zugriff stets nach dem Prinzip der geringsten Berechtigung zu beschränken; so hat z. B. nur ein Benutzer mit der Rolle "Setup" das Recht, bestimmte Einstellungen zu ändern. Benutzer, die während des normalen Betriebs aktiv sind, müssen auf das notwendige Minimum an Rechten beschränkt sein, um die Auswirkungen möglicher Sicherheitsvorfälle zu begrenzen

KEBA © KEBA 2021

KeControl und KeTop Geräte unterstützen das KEBA-Authentifizierungsmanagement. Übersichtliche und einfach zu bedienende Benutzeroberflächen für das Authentifizierungsmanagement verhindern Fehler mit gravierenden Sicherheitsfolgen. KeStudio und DevAdmin sind die Schnittstellen für das Authentifizierungsmanagement dieser Geräte.

Die Nutzung des Authentifizierungsmanagements des Betriebssystems ist bei ausgewählten Produkten ebenfalls möglich. Dieses Kapitel befasst sich nur mit dem KEBA-Authentifizierungsmanagement. Das betriebssystemspezifische Authentifizierungsmanagement ist in den Benutzerhandbüchern der Betriebssysteme dokumentiert.

Die Authentifizierungsverwaltung umfasst die Verwaltung der Benutzerkonten und der zugewiesenen Kennungen und Authentifikatoren. Bei der Authentifizierung geht es aber nicht nur um Benutzer. Zur Authentifizierung gehört auch die Verwaltung von dienstespezifischen Schlüsseln und Zertifikaten.

Benutzerverwaltung

Mit der KEBA-Benutzerverwaltung können Benutzer angelegt, konfiguriert und gelöscht werden. Zusätzlich können Rollen angelegt, konfiguriert und gelöscht werden. Diese Rollen können den Benutzern zugewiesen werden. Einem einzelnen Benutzer können mehrere Rollen zugewiesen werden. Benutzer mit Rollen können sich zwar authentifizieren, dürfen aber trotzdem nichts tun, wenn diesen Rollen keine Rechte zugewiesen sind. Diese Rechte sind vordefiniert und können weder erstellt noch gelöscht werden. Sie werden von der Software verwendet, um zu entscheiden, ob der Zugriff gewährt wird oder nicht. Einer einzelnen Rolle können mehrere Rechte zugewiesen werden. Außerdem können Benutzereinstellungen und Metadaten konfiguriert werden.

Jeder Benutzer benötigt eine eindeutige Kennung. Für die KEBA-Benutzerverwaltung ist die eindeutige Kennung der Benutzername. Es wird dem Benutzer keine zusätzliche ID zugewiesen. Passwörter werden als Authentifikator für alle Benutzer verwendet.

Für KEBA-Geräte gibt es einen Standardbenutzer namens "Administrator", dem die Standardrolle "Administrator" zugewiesen ist. Der Benutzer "Administrator" kann umbenannt werden, die Rolle "Administrator" jedoch nicht. Die Standardrolle "Administrator" ist mit allen Rechten belegt. So ist der Zugriff auf die Benutzerverwaltung selbst für diese Rolle immer gegeben. Der Benutzer mit dieser Rolle ist also der Schlüssel zum gesamten Gerät. Das Passwort für mindestens einen Benutzer mit der Rolle "Administrator" sollte gesetzt werden, da sonst nachträglich kein Benutzerzugang freigeschaltet werden kann und ein Zugriff aus dem Automatisations-Netzwerk nicht möglich ist. Ein Standard-Passwort gibt es nicht. Weitere Standardbenutzer, die existieren können, sind "Operator", "Service" und "Teacher".

Standardrollen

Rollen benötigen Rechte, um den Zugriff tatsächlich zu ermöglichen. Die Rechte sind feinkörnig, um eine genaue Zuweisung der Mindestrechte an Rollen und Benutzer zu ermöglichen. Um den Benutzern die Auswahl der

© KEBA 2021

Rechte zu erleichtern, sind vordefinierte Standardrollen verfügbar. Diesen Standardrollen ist ein eigener Satz von Rechten zugewiesen, der auf die Aufgabe der Rolle abgestimmt ist. Normalerweise können Benutzer nur mit diesen Standardrollen modelliert werden. Die Liste der Standardrollen ist kurz gehalten, um das Verständnis und die Verwendung der Rollen zu erleichtern. Die verfügbaren Standardrollen sind:

- **Configuration**: Diese Rolle erlaubt den Zugriff auf alle Konfigurationen, die notwendig sind, um das Gerät in eine Umgebung zu integrieren. Diese Konfigurationen müssen den Anforderungen der Umgebung entsprechen und können nicht willkürlich und ohne Konsequenzen eingestellt werden. Diese Rolle erlaubt die Grundkonfiguration einer Maschine, die kein maschinenspezifisches Know-how erfordert. Sie umfasst keine anwendungs- oder maschinenspezifischen Konfigurationen. Beispiele hierfür sind Einstellungen im Zusammenhang mit dem Automatisations-Netzwerk wie die IP-Adresse des Automatisations-Netzwerks und die Konfiguration des Zeitservers.
- **Setup**: Die "Setup"-Rolle erlaubt umfangreichere Konfigurationen als die "Configuration"-Rolle. Sie erlaubt alles, was nicht von der Rolle "Configuration" abgedeckt wird, mit Ausnahme der Benutzerverwaltung. Die "Setup"-Rolle ermöglicht den Zugriff auf anwendungs- und gerätespezifische Einstellungen. Außerdem sind Softwareinstallation, -Updates und -Backups erlaubt und die Anwendung kann geändert werden. Konfigurationen, die sich auf das Maschinen-Netzwerk beziehen, sind anwendungs-/maschinenspezifisch und werden daher von dieser Rolle abgedeckt. Weitere Beispiele sind die Firewall-Konfiguration und die Aktualisierung der Firmware.
- **Access**: Die "Access"-Rolle ermöglicht die Verwaltung von Benutzern und Rollen sowie die Zuweisung von Rechten an Rollen. Wenn ein Benutzer diese Rolle hat, dann hat er faktisch alle Rechte, denn er kann sich selbst alle Rechte zuweisen. Es handelt sich also um eine spezielle Rolle, die nur wenigen, idealerweise nur einem Benutzer zugewiesen wird.
- **Application**: Diese Rolle ermöglicht den Zugriff auf alle Variablen und Aktionen, die während des Betriebs benötigt werden. Idealerweise wird nur diese Rolle an Benutzer vergeben, um dem Prinzip des geringsten Privilegs zu folgen. Da Benutzer mit dieser Rolle permanent aktiv sein können, verringert sich das Sicherheitsrisiko, wenn nicht auch andere Rollen und Rechte potentiell permanent verfügbar sind. Beispiele, bei denen diese Rolle verwendet werden sollte, sind SCADA-Systeme oder andere Geräte, die im Betrieb über Web-Interfaces kommunizieren.
- **Development**: Mit dieser Rolle haben Sie Zugriff auf alles, was für die Anwendungsentwicklung erforderlich ist. Anwendungsdownload, -ausführung und -debugging sind inbegriffen. Alle Arten von Anwendungen wie IEC, XCRT und Visualisierungen sind erlaubt.
- **Diagnosis**: Die "Diagnosis"-Rolle soll den einfachen Zugriff auf Diagnosedaten ermöglichen. Diese Rolle erlaubt keine Änderungen und kann sicher einem breiten Benutzerkreis zugewiesen werden. Mit der Diagnoserolle können Softwareversionen und Typenschilder gelesen, die konfi-

KEBA © KEBA 2021

gurierten und verfügbaren Geräte aufgelistet, der Steuerung-Trace gelesen, Statusmeldungen ausgelöst und kopiert sowie verschiedene andere Informationen abgerufen werden.

- **Visualisation**: Diese Rolle ermöglicht den Zugriff auf Visualisierungen über das Netzwerk. Die Funktionen, die eine Visualisierung bietet, können sehr breit gefächert sein und hängen von der jeweiligen Anwendung ab. Daher sind generische Rollen nicht geeignet und diese spezifische Rolle wird verwendet.

Die obige Liste gibt nur einen Überblick darüber, was mit einer bestimmten Rolle und den ihr zugewiesenen Rechten gemacht werden kann. Die genauen erforderlichen Rechte für bestimmte Informationen, Aktionen und Schnittstellen sind in den Benutzerhandbüchern dokumentiert.

Schlüssel- und Zertifikatsverwaltung

Bei der Authentifizierung geht es nicht nur um Benutzer und Kennwörter. Es werden auch Schlüssel verwendet, z. B. für die Authentifizierung von SSH-Benutzern. Außerdem werden häufig Zertifikate für die gegenseitige Authentifizierung von Diensten verwendet. Zertifikate enthalten öffentliche Schlüssel und werden mit privaten Schlüsseln signiert. Schlüssel und Zertifikate müssen generiert werden. Ihr Format und ihre Eigenschaften sind spezifisch für die Dienste, für die sie verwendet werden. Dies macht die manuelle Generierung von Schlüsseln und Zertifikaten zu einer schwierigen Aufgabe mit vielen möglichen Fehlern. Daher unterstützt das KEBA-Authentifizierungsmanagement die Generierung von Schlüsseln und Zertifikaten. Einige Schlüssel und Zertifikate werden beim ersten Booten eines Gerätes erzeugt. Andere Schlüssel und Zertifikate werden bei Bedarf über die Benutzeroberfläche DevAdmin generiert. Für ausgewählte Dienste ist die Installation statt der Generierung von Schlüsseln und Zertifikaten möglich.

Öffentliche Schlüssel und Zertifikate können vorinstalliert werden. Dies ist für die Authentifizierung und Überprüfung von Daten erforderlich. Dies stellt kein Sicherheitsrisiko dar, da öffentliche Schlüssel und Signaturen keine Geheimnisse sind, die vertraulich behandelt werden müssen. Private Schlüssel hingegen sind Geheimnisse. Daher werden private Schlüssel nie vorinstalliert und es werden keine Standardschlüssel verwendet

1.3.2.6 Dienste für das Automationsnetzwerk

KEBA-IACS-Komponenten sind in der Lage, dem Automatisations-Netzwerk verschiedene Dienste mit spezifischen Sicherheitseigenschaften zur Verfügung zu stellen. Diese spezifischen Sicherheitseigenschaften müssen bekannt sein, um zu entscheiden, ob ein Dienst verwendet werden soll und wie er konfiguriert wird, um die erforderliche Sicherheitsstufe zu bieten. In der Produktdokumentation wird angegeben, ob ein bestimmter Dienst unterstützt wird oder nicht.

Web-Interface

Das Web-Interface bietet eine umfangreiche Sammlung von RESTful und WebSocket (WS) APIs für nahezu alle Funktionen der KEBA-IACS-Komponenten. KeControl- und KeTop-Geräte unterstützen das Web-Interface. Beispiele für APIs sind:

© KEBA 2021

- Variablen Service
- Geräte Service
- Datei Service
- Zugriff service
- Konfiguration
- ...

HTTPS ist das sichere Protokoll, das für die Webschnittstelle verwendet wird. HTTP wird ebenfalls unterstützt, sollte aber auf das Maschinen-Netzwerk beschränkt werden und muss explizit aktiviert werden. Falls erforderlich, ermöglicht die Firewall die Beschränkung von HTTP auf das Maschinen-Netzwerk für "Boundary protection devices", wenn HTTP nicht ausgeschaltet werden kann.

Für die Nutzung der Web-Schnittstelle ist eine Authentifizierung erforderlich. Die Authentifizierung erfolgt auf Basis der KEBA-Benutzerverwaltung. Je nach den Rechten, die den Rollen der Benutzer zugewiesen sind, wird der Zugriff auf APIs erlaubt oder nicht. Insbesondere der Zugriff auf die Zugriffsdienst-API für die Authentifizierungsverwaltung soll nur einem minimalen Satz von Rollen und Benutzern gestattet werden, da Authentifizierungseinstellungen und Passwörter über diese API geändert werden können. Benutzer mit der Rolle "Administrator" haben Zugriff auf die gesamte Web-Schnittstelle einschließlich der Zugriffsdienst-API. Benutzer ohne irgendwelche für die Web-Schnittstelle relevanten Rechte haben keinen Zugang zur Webschnittstelle.

Wenn beim Einrichten des Ziels in KeStudio kein Zertifikat konfiguriert wird, wird beim ersten Hochlauf ein Zertifikat generiert. Dieses Zertifikat ist selbstsigniert und läuft nach 90 Tagen ab. Die Prüfung auf signierte und nicht abgelaufene Zertifikate muss im HTTPS-Client deaktiviert werden, wenn dieses generierte Zertifikat verwendet wird. Dieses generierte Zertifikat bietet ein geringeres Sicherheitsniveau als ein signiertes Zertifikat, das regelmäßig vor Ablauf der Gültigkeit ausgetauscht wird. Die Authentifizierung des Servers ist schwächer, aber die Verschlüsselung der Kommunikation ist gleich.

Wenn das bestehende, generierte Zertifikat ungültig wird, wird erneut ein neues Zertifikat generiert. Dies geschieht z. B., wenn eine IP-Adresse des Geräts geändert wird, da das generierte Zertifikat die IP-Adressen des Geräts im Zertifikat aufführt. Dies ist bei konfigurierten Zertifikaten nicht der Fall. Konfigurierte Zertifikate werden niemals durch generierte Zertifikate ersetzt.

Dienst	Web-Schnittstelle
Server-Authentifizierung	Zertifikat (nur für HTTPS)
Client-Authentifizierung	Benutzer/Passwort
Ablauf des Zertifikats	ja
Zugangsrechte	KEBA-Benutzerverwaltung

KEBA © KEBA 2021

DevAdmin

Der DevAdmin ist eine webbasiertes Obefläche, das den Zugriff auf verschiedene Informationen und Aktionen der KEBA-IACS-Komponenten ermöglicht. KeControl und KeTop Geräte unterstützen den DevAdmin. HTTPS ist das von DevAdmin verwendete sichere Protokoll, HTTP ist nur optional. Der DevAdmin basiert auf dem Web-Interface und bietet identische Sicherheitseigenschaften:

Dienst	Web-Interface
Server-Authentifizierung	Zertifikat (nur für HTTPS)
Client-Authentifizierung	Benutzer/Passwort
Ablauf des Zertifikats	ja
Zugangsrechte	KEBA-Benutzerverwaltung

Secure-Shell

Secure Shell (SSH) wird von Linux-basierten KeControl- und KeTop-Geräten bereitgestellt. Root-Login und Passwort-Authentifizierung sind deaktiviert, um ein hohes Standard-Sicherheitsniveau zu gewährleisten. Es gibt die folgenden SSH-Benutzer:

- **admin**: Der Benutzer "admin" hat die volle Kontrolle über das Gerät. Er ist nicht der root-Benutzer, darf aber mit "`sudo su -`" eine root-Shell öffnen. Der SSH-Schlüssel für den Benutzer "admin" kann während der Einrichtung des Targets mit KeStudio oder nachträglich mit DevAdmin konfiguriert werden (Rolle "Administrator" erforderlich).
- **service**: Der Benutzer "service" hat Zugriff auf ausgewählte Dateien und Verzeichnisse, z. B. um auf die Protokolldaten des Rechners zuzugreifen. Dieser Benutzer hat keinen Shell-Zugriff, nur Dateizugriff ist möglich. Der SSH-Schlüssel für den "service"-Benutzer kann bei der Targeteinrichtung mit KeStudio, anschließend mit DevAdmin (Rolle "Administrator" erforderlich) oder durch Dateizugriff auf die Datei mit den autorisierten Schlüsseln konfiguriert werden.
- **operator**: Der Benutzer "operator" hat Zugriff auf ausgewählte Dateien und Verzeichnisse. Standardmäßig sind keine Dateien oder Verzeichnisse zugänglich. Die zugänglichen Dateien und Verzeichnisse können mit KeStudio konfiguriert werden. Der SSH-Schlüssel für den "operator"-Benutzer kann bei der Targeteinrichtung mit KeStudio oder nachträglich mit DevAdmin (Rolle "Administrator" erforderlich) konfiguriert werden.

SSH-Schlüssel haben keine Verfallszeit. Sie sind so lange gültig, bis sie durch neue Schlüssel ersetzt werden. Das regelmäßige Ersetzen der SSH-Schlüssel durch neue ist möglich und würde das Risiko einer Schlüsselkompromittierung verringern.

Die SSH-Sicherheitseigenschaften sind:

Dienst	SSH
Server-Authentifizierung	Host-Schlüssel (wird beim ersten Start erzeugt)

© KEBA 2021

Dienst	SSH
Client-Authentifizierung	Privater Schlüssel (öffentlicher Schlüssel auf dem Host gespeichert)
Ablauf des Schlüssels	Nein
Zugangsrechte	Shell- und Dateizugriff individuell pro Benutzer eingeschränkt

OpenVPN

OpenVPN ermöglicht den Zugriff auf das Maschinen-Netzwerk, ohne dass ein physischer Zugang zum Maschinen-Netzwerk erforderlich ist. Die OpenVPN-Authentifizierung ersetzt den physischen Zugang zum Schrank. In der Regel läuft der OpenVPN-Dienst auf dem "Boundary protection device". KeControl- und KeTop-Geräte sind in der Lage, als Boundary-Protection-Geräte zu fungieren und unterstützen somit OpenVPN.

Client und Server einer OpenVPN-Verbindung authentifizieren sich gegenseitig. Zur Authentifizierung prüfen beide das Zertifikat des anderen auf eine gültige Certificate Authority (CA) Signatur. Daher muss das CA-Zertifikat auf beiden vorhanden sein, um die Signaturprüfung zu ermöglichen. Der private Schlüssel der CA ist notwendig, um das Zertifikat von Client und Server zu signieren.

Für OpenVPN werden die notwendigen Schlüssel und Zertifikate beim ersten Booten erzeugt. Zuerst werden der private Schlüssel und das Zertifikat der CA generiert. Danach werden der private Schlüssel und das Zertifikat des Servers generiert und das Zertifikat wird mit dem privaten Schlüssel der CA signiert. Um eine OpenVPN-Verbindung zu ermöglichen, ist ein von der CA signiertes Client-Zertifikat erforderlich. Dieses Client-Zertifikat wird bei Bedarf generiert. Die Client-Zertifikate können mit DevAdmin verwaltet werden.

Die höchste Sicherheitsstufe für OpenVPN wird erreicht, wenn der private Schlüssel der CA nicht auf dem OpenVPN-Server gespeichert ist. In diesem Fall würden die Server- und Client-Zertifikate in einer geschützten Umgebung mit Zugriff auf den privaten Schlüssel der CA signiert werden. Diese Praxis würde eine Schlüsselverwaltung außerhalb der KEBA-Geräte und eine manuelle Bereitstellung der Schlüssel und Zertifikate erfordern.

Wenn die OpenVPN-Schlüssel und -Zertifikate generiert werden, dann wird der private Schlüssel der CA auf dem Server gespeichert, auf den auch die OpenVPN-Verbindung zugreift. Daher ist das Sicherheitsniveau im Vergleich zu einer externen Schlüsselverwaltung niedriger, aber es bietet immer noch Authentifizierung und Verschlüsselung der OpenVPN-Verbindung.

OpenVPN-Zertifikate laufen ab. Kurze Verfallszeiten bieten ein hohes Sicherheitsniveau, aber auch einen hohen Wartungsaufwand. Generierte Schlüssel und Zertifikate sollen eine einfache Nutzung der Sicherheitsfunktionen ermöglichen. Daher sind die Ablauffristen des Servers und des CA-Zertifikats auf 100 Jahre gesetzt, um ein Ablaufen in der Praxis zu verhindern. Die Client-Zertifikate verfallen standardmäßig nach 90 Tagen. Dieser Zeitraum kann auf bis zu 50 Jahre erhöht werden. Dies ermöglicht die Nutzung von OpenVPN, ohne dass man sich Gedanken über die Wartung der Sicherheit machen muss.

KEBA © KEBA 2021

Die OpenVPN-Sicherheitseigenschaften sind:

Dienst	Web-Interface
Server-Authentifizierung	Zertifikat
Client-Authentifizierung	Zertifikat
CA-Authentifizierung	Zertifikat
Ablauf des Zertifikats	Ja
Zugangsrechte	Wie Maschninen-Netzwerkzugang

OPC-Unified-Architecture

OPC-Unified-Architecture (OPC-UA) ist eine plattformunabhängige, serviceorientierte Architektur für die industrielle Automatisierung und Kommunikation. Sie ist die neueste Spezifikation des Open-Platform-Communications-(OPC)-Standards, der den sicheren und zuverlässigen Datenaustausch zwischen Maschinen, Geräten und Anlagen unterschiedlicher Hersteller ermöglichen soll. Er kann für den Datenaustausch im Betrieb und zur Diagnose verwendet werden. OPC-UA wird vor allem in Automatisations-Netzwerken, aber auch in Maschinen-Netzwerken eingesetzt. Es unterstützt eine sichere Kommunikation mit Authentifizierung und Verschlüsselung.

OPC-UA erfordert eine Authentifizierung mit Benutzernamen und Passwort. Diese Authentifizierung basiert auf der KEBA-Benutzerverwaltung. Anhand von Rollen, die den Benutzern zugewiesen werden, wird der Zugriff auf Objekte und Variablen gewährt oder nicht. Die oben erwähnten Rechte der Authentifizierungsverwaltung werden für die OPC-UA Zugriffskontrolle nicht verwendet. OPC-UA-spezifische Berechtigungen werden den Rollen individuell zugewiesen und diese Berechtigungen werden bei jedem Zugriff überprüft. Dies ermöglicht eine feinkörnige Zugriffskontrolle, die sicherstellt, dass nur autorisierte Benutzer auf bestimmte Daten zugreifen und bestimmte Handlungen durchführen können.

Zusätzlich zu Benutzername und Passwort gibt es eine weitere Authentifizierungsschicht auf der Basis von Zertifikaten, die auch Verschlüsselung unterstützt. OPC-UA verwendet Zertifikate für die Authentifizierung sowohl des Clients als auch des Servers. Das Zertifikat des Kommunikationspartners muss bekannt sein. Der Kommunikationspartner muss den Besitz des Zertifikats nachweisen. Dieser Nachweis ist nur möglich, wenn der Kommunikationspartner den zugehörigen privaten Schlüssel kennt. Dies gilt für Client und Server. Z.B. speichert der Server das Zertifikat des Clients und der Client weist den Besitz des Zertifikats nach. Die Zertifikate enthalten eine Anwendungs-URI. Diese Anwendungs-URI wird für Informationszwecke verwendet, z. B. zur Auflistung der verbundenen Clients. Die Signatur der Zertifikate wird nicht validiert, es können selbstsignierte Zertifikate verwendet werden.

Auf der Grundlage der gegenseitigen Authentifizierung mit Zertifikaten wird eine sichere Kommunikation aufgebaut. Diese sichere Kommunikation ist in der Regel verschlüsselt und signiert, was vor Abhören und Manipulation schützt. Optional kann die Verschlüsselung auch entfallen. Wird keine Verschlüsselung verwendet, wird die Kommunikation dennoch signiert und die Integrität geschützt, d. h. Datenmanipulationen werden erkannt.

© KEBA 2021

Für den OPC-UA Server wird ein Zertifikat benötigt. Wenn kein Zertifikat für den Server konfiguriert ist, ist der OPC-UA Server nicht verfügbar. Das Zertifikat kann mit DevAdmin installiert oder generiert werden.

Der OPC-UA Client ist in der Lage, mehrere Zertifikate zu verwenden. Dies ist notwendig, da sich ein OPC-UA Client potentiell mit mehreren Servern verbindet und es keine Garantie dafür gibt, dass alle Server das gleiche Zertifikat akzeptieren können. Die Zertifikate können mit DevAdmin installiert und verwaltet werden. Die Konfiguration von Benutzername/Passwort-Kombinationen, die auch für die Authentifizierung an OPC-UA Servern notwendig sind, erfolgt zusammen mit der gesamten OPC-UA Client Konfiguration in KeStudio.

Für den Substandard OPC-UA-PubSub sind Authentifizierung und Verschlüsselung zwar spezifiziert, aber noch nicht implementiert. Daher wird von der Verwendung von OPC-UA-PubSub innerhalb des Automatisations-Netzwerks dringend abgeraten. OPC-UA-PubSub soll nur noch innerhalb des Maschinen-Netzwerkes verwendet werden.

Weitere Details zu den OPC-UA Sicherheitsfunktionen kann der OPC-UA Produktdokumentation entnommen werden.

Dienst	OPC-UA
Server-Authentifizierung	Zertifikat
Client-Authentifizierung	Benutzer/Passwort, Zertifikat
Ablauf des Zertifikats	Ja
Zugangsrechte	KEBA-Benutzerverwaltung, OPC-UA spezifische Berechtigungen auf Basis von Rollen

1.3.2.7 Dienste für das Maschinennetzwerk

Das Maschinen-Netzwerk ist ein internes Netz der Maschine oder der Anlage selbst. Es ist von allen anderen Netzwerken durch einen "Boundary protection device" isoliert. In der Regel gibt es ein einziges "Boundary protection device", das das Maschinen-Netzwerk mit dem Automatisations-Netzwerk verbindet. Gibt es kein "Boundary protection device", so gibt es auch kein Maschinen-Netzwerk und die für das Maschinen-Netzwerk vorgesehenen Dienste dürfen nicht genutzt werden.

Das Maschinen-Netzwerk ist eine vertrauenswürdige Zone. Gemäß der "Defense in Depth"-Sicherheitsstrategie muss es durch mehrere Schichten von Firewalls und "Boundary protection devices" geschützt werden. Darüber hinaus sind physische Zugangsbeschränkungen zu den Produktionsräumen und noch restriktiver zum Schaltschrank erforderlich. Diese Maßnahmen lassen die folgenden Annahmen zu:

- Die Wahrscheinlichkeit für das logische und physische Vorhandensein von nicht autorisierten Geräten ist so gering, dass auf eine Authentifizierung und Autorisierung verzichtet werden kann.
- Die Kommunikation innerhalb des Maschinen-Netzwerkes erfolgt nicht über nicht vertrauenswürdige Kanäle oder Verbindungen. Daher ist eine Verschlüsselung für die Kommunikation innerhalb des Maschinen-Netzwerkes nicht erforderlich.

KEBA © KEBA 2021

Zuverlässigkeit und Integrität sind die Ziele mit der höchsten Priorität für ein IACS. Wäre das Maschinen-Netzwerk eine nicht-vertrauenswürdige Zone, so könnte die geforderte Zuverlässigkeit nicht erreicht werden. So können z.B. definierte Reaktionszeiten nicht garantiert werden, wenn gleichzeitig bösartiger Verkehr im Maschinen-Netzwerk vorhanden ist. Auch die physikalische Verkabelung muss vertrauenswürdig sein, um die geforderte Integrität zu erreichen. Daher ist es notwendig, die Maschine oder das System und damit auch das Maschinen-Netzwerk als vertrauenswürdige Zone zu implementieren. Somit bietet das Maschinen-Netzwerk von vornherein ein höheres Sicherheitsniveau, und die Sicherheitsanforderungen für Dienste innerhalb des Maschinen-Netzwerkes sind im Vergleich zum Automatisations-Netzwerk geringer.

KEBA KeControl- und KeTop-Geräte können als "Boundary protection devices" für Maschinen-Netzwerke eingesetzt werden. In diesem Fall muss die Firewall so konfiguriert werden, dass nur sichere Dienste für das Automatisations-Netzwerk zur Verfügung stehen. Andere, nicht sichere Dienste werden dann nur für das Maschinen-Netzwerk bereitgestellt.

Wenn ein Maschinen-Netzwerk mit einem "Boundary protection device" vorhanden ist, dann ist die Nutzung der unten aufgeführten Dienste innerhalb dieses Netzes erlaubt. Die oben aufgeführten Dienste des Automatisations-Netzwerkes können auch im Maschinen-Netzwerk verwendet werden, da die Sicherheitsanforderungen für das Maschinen-Netzwerk geringer sind als für das Automatisations-Netzwerk.

Jeder Maschinen-Netzwerkdienst, der von KEBA IACS-Komponenten bereitgestellt wird, hat spezifische Sicherheitseigenschaften. Diese spezifischen Sicherheitseigenschaften müssen bekannt sein, um zu entscheiden, ob ein Dienst verwendet werden soll und wie er konfiguriert wird, um die erforderliche Sicherheitsstufe zu bieten. In der Produktdokumentation wird angegeben, ob ein bestimmter Dienst unterstützt wird oder nicht.

Feldbusse

Feldbusse werden nur innerhalb von Maschinen-Netzwerken verwendet. Es gibt verschiedene Arten von Feldbussen, aber sie haben gemeinsame Eigenschaften. Feldbusgeräte werden nur identifiziert und nicht authentifiziert. Die Kommunikation ist nicht verschlüsselt und muss Echtzeiteigenschaften erfüllen. Da das Maschinen-Netzwerk eine vertrauenswürdige Zone ist, ist die Verwendung von Feldbussen auch ohne fortgeschrittene Sicherheitsmaßnahmen zulässig.

Die Kommunikation auf Feldbussen ist in der Regel auf ein Minimum reduziert, was der Sicherheit zugute kommt. Der Inhalt der Kommunikation muss konfiguriert werden und kann nicht willkürlich zur Laufzeit erweitert werden. Damit entspricht diese Konfiguration dem Prinzip der geringsten Privilegien.

Einige Feldbusse unterstützen Ethernet-basierte Kommunikation, z. B. unterstützt EtherCAT EoE (Ethernet over EtherCAT). Diese Ethernet-basierte Kommunikation muss auf das Maschinen-Netzwerk beschränkt werden. KEBA-"Boundary protection devices" wie KeControl- und KeTop-Produkte beschränken diese Ethernet-basierte Kommunikation auf das Maschinen-Netzwerk.

© KEBA 2021

Die Sicherheitseigenschaften für Feldbusse sind:

Dienst	Anzeige- und Bedienelemente
Authentifizierung der Anwendung	Geografischer Standort, Maschinen-Netzwerk
Zugangsrechte	Keine Einschränkungen

RPC

KeControl und KeTop bieten RPC-basierte Dienste. Diese RPC-basierten Dienste bieten eine breite Palette von Funktionen, die von diesen Geräten unterstützt werden. Alle diese Dienste sind KEBA-spezifisch, nur RPC selbst ist ein standardisiertes Protokoll ("Remote Procedure Call")

Das RPC-Protokoll unterstützt keine Sicherheitsmerkmale wie Authentifizierung und Verschlüsselung. Daher sollte die Verwendung von RPC und der darauf basierenden Dienste auf eine vertrauenswürdige Zone wie das Maschinen-Netzwerk beschränkt werden. Von der Verwendung von RPC und den darauf basierenden Diensten innerhalb des Automatisations-Netzwerkes oder eines anderen Netzes ohne zusätzliche Sicherheitsmaßnahmen wird dringend abgeraten.

KEBA-Tools wie KeStudio verwenden RPC zur Kommunikation mit KEBA-Geräten. Wenn das RPC-Protokoll z.B. durch eine Firewall auf das Maschinen-Netzwerk beschränkt ist, dann ist die Kommunikation der Tools nur möglich, wenn die Toolsoftware Zugriff auf das Maschinen-Netzwerk hat; z.B. der Laptop mit der KeStudio-Installation ist mit dem "Ethernet 1"-Port des KeControl-Gerätes verbunden. Mit OpenVPN kann auch ohne physikalischen Zugang auf das Maschinen-Netzwerk zugegriffen werden. In diesem Fall ist OpenVPN die zusätzliche Sicherheitsmaßnahme, die die Verwendung von RPC in anderen Netzwerken als dem Maschinen-Netzwerk ermöglicht.

Die RPC-Sicherheitseigenschaften sind:

Dienst	Anzeige- und Bedienelemente
Authentifizierung der Anwendung	Geografischer Standort, Maschinen-Netzwerk
Benutzerauthentifizierung	Geografischer Standort, Maschinen-Netzwerk
Zugangsrechte	Keine Einschränkungen

KVC

Das KVC-Protokoll ist ein KEBA-spezifisches Protokoll für die Kommunikation zwischen KeControl-Geräten und KeTop-Geräten. KVC ist die Abkürzung für "KEBA Virtual Channel". Dieser virtuelle Kanal wird verwendet, um:

- Den Status der KeTop-Schlüssel abzufragen
- Den Status der KeTop-LEDs zu setzen
- Die Ausrichtung des KeTop-Geräts zu ermitteln
- Den Status des KeTop-Handrads abzufragen

KEBA © KEBA 2021

- ...

Das KVC-Protokoll unterstützt keine Sicherheitsmerkmale wie Authentifizierung und Verschlüsselung. Daher sollte die Verwendung von KVC auf eine vertrauenswürdige Zone wie das Maschinen-Netzwerk beschränkt werden. Von der Nutzung dieses Dienstes innerhalb des Automatisations-Netzwerkes oder eines anderen Netzes wird dringend abgeraten.

Die KVC-Sicherheitseigenschaften sind:

Dienst	Anzeige- und Bedienelemente
Authentifizierung der Anwendung	geografischer Standort, Maschinen-Netzwerk
Zugangsrechte	keine Einschränkungen

CODESYS

KeControl und eine begrenzte Anzahl von KeDrive-Geräten unterstützen das CODESYS-Laufzeitsystem. Für die Kommunikation mit dem CODESYS-Laufzeitsystem wird ein bestimmter Satz von Kommunikationsprotokollen verwendet. Dieser Satz wird als CODESYS-Kommunikationsprotokolle bezeichnet.

Die CODESYS-Kommunikationsprotokolle unterstützen die Authentifizierung. Verschlüsselung wird nicht verwendet. Daher sollte die Verwendung der CODESYS-Kommunikationsprotokolle auf eine vertrauenswürdige Zone wie das Maschinen-Netzwerk beschränkt werden. Von der Verwendung von CODESYS-Kommunikationsprotokollen innerhalb des Automatisations-Netzwerks oder eines anderen Netzwerks ohne zusätzliche Sicherheitsmaßnahmen wird dringend abgeraten.

KEBA-Tools wie KeStudio verwenden die CODESYS-Kommunikationsprotokolle zur Kommunikation mit KEBA-Geräten mit CODESYS-Laufzeit. Wenn die CODESYS-Kommunikationsprotokolle z.B. durch eine Firewall auf das Maschinen-Netzwerk beschränkt sind, dann ist die Kommunikation der Tools nur möglich, wenn die Toolsoftware Zugriff auf das Maschinen-Netzwerk hat; z.B. der Laptop mit der KeStudio-Installation ist mit dem "Ethernet 1"-Port des KeControl-Gerätes verbunden. Mit OpenVPN kann auch ohne physikalischen Zugang auf das Maschinen-Netzwerk zugegriffen werden. In diesem Fall ist OpenVPN die zusätzliche Sicherheitsmaßnahme, die die Verwendung von CODESYS-Kommunikationsprotokollen in anderen Netzwerken als dem Maschinen-Netzwerk ermöglicht.

Die Sicherheitseigenschaften der CODESYS-Kommunikationsprotokolle sind:

Dienst	Anzeige- und Bedienelemente
Benutzerauthentifizierung	Benutzer/Passwort
Zugangsrechte	Keine Einschränkungen

© KEBA 2021

EtherCAT-Mailbox-Gateway

Der EtherCAT-Mailbox-Gateway-Dienst ermöglicht den Zugriff auf die Mailbox von EtherCAT-Slaves. Dieser direkte Zugriff wird in der Regel genutzt, um EtherCAT-Slaves mit funktionalen Sicherheitsmerkmalen zu konfigurieren. In diesem Fall wird das AoE-Mailbox-Protokoll verwendet.

Das EtherCAT-Mailbox-Gateway-Protokoll unterstützt keine Sicherheitsfunktionen wie Authentifizierung und Verschlüsselung. Daher sollte die Verwendung des EtherCAT Mailbox-Gateways auf eine vertrauenswürdige Zone wie das Maschinen-Netzwerk beschränkt werden. Von der Nutzung dieses Dienstes innerhalb des Automatisations-Netzwerks oder eines anderen Netzwerks ohne zusätzliche Sicherheitsmaßnahmen wird dringend abgeraten.

KEBA-Tools wie KeStudio SafeEdit NG verwenden das EtherCAT-Mailbox-Gateway zur Kommunikation mit KEBA-Geräten der funktionalen Sicherheit. Ist das EtherCAT Mailbox-Gateway z.B. durch eine Firewall auf das Maschinen-Netzwerk beschränkt, so ist die Kommunikation dieser Tools nur möglich, wenn KeStudio SafeEdit NG Zugriff auf das Maschinen-Netzwerk hat; z.B. wenn der Laptop mit der KeStudio SafeEdit NG-Installation mit dem "Ethernet 1"-Port der KeControl verbunden ist. OpenVPN oder andere sichere Tunnel wie SSH können verwendet werden, um Zugriff auf das Maschinen-Netzwerk ohne physischen Zugang zu erhalten. In diesem Fall ist der sichere Tunnel die zusätzliche Sicherheitsmaßnahme, die die Verwendung von RPC in anderen Netzwerken als dem Maschinen-Netzwerk ermöglicht.

Die Sicherheitseigenschaften des EtherCAT-Mailbox-Gateways sind:

Dienst	Anzeige- und Bedienelemente
Authentifizierung der Anwendung	Geografischer Standort, Maschinen-Netzwerk
Benutzerauthentifizierung	Geografischer Standort, Maschinen-Netzwerk
Zugangsrechte	Keine Einschränkungen

Steuerung-Protokolle für Fremd-Steuerungen (nicht-KEBA-Steuerungen)

Für die Kommunikation von KeTop-Geräten mit Fremd-Steuerungen werden mehrere Protokolle unterstützt:

- ADS (Beckhoff-Steuerung)
- S7 (Siemens-Steuerung)
- Modbus

Ähnlich wie bei KVC werden diese Protokolle verwendet, um:

- Den Status der KeTop-Schlüssel abzufragen
- Den Status der KeTop-LEDs zu setzen
- Die Ausrichtung des KeTop-Geräts zu ermitteln
- Den Status des KeTop-Handrads abzufragen

KEBA © KEBA 2021

- ...

Diese Steuerung-Protokolle für Fremd-Steuerungen von Drittanbietern unterstützen keine Sicherheitsmerkmale wie Authentifizierung und Verschlüsselung. Daher sollte die Verwendung dieser Protokolle auf eine vertrauenswürdige Zone wie das Maschinen-Netzwerk beschränkt werden. Von der Verwendung von Steuerung-Protokolle für nicht-KEBA-Steuerungen innerhalb des Automatisations-Netzwerkes oder eines anderen Netzes wird dringend abgeraten.

Die Sicherheitseigenschaften von Steuerung-Protokolle für Fremd-Steuerungen sind:

Dienst	Anzeige- und Bedienelemente
Authentifizierung der Anwendung	Geografischer Standort, Maschinen-Netzwerk
Benutzerauthentifizierung	Geografischer Standort, Maschinen-Netzwerk
Zugangsrechte	Keine Einschränkungen

1.3.2.8 Drahtlose Schnittstellen

Neben drahtgebundenen Schnittstellen wie Ethernet und CAN werden für ausgewählte KEBA IACS Komponenten auch drahtlose Schnittstellen unterstützt. Besonderes Augenmerk ist auf die Sicherheit der drahtlosen Schnittstellen zu legen, da eine physikalische Zugriffsbeschränkung bei dieser Art von Schnittstellen nicht immer möglich ist.

RFID

Ausgewählte KEBA IACS-Komponenten verfügen über eine RFID-Schnittstelle, um Informationen von RFID-Karten zu lesen. Diese Informationen werden in der Regel zur Benutzerauthentifizierung verwendet und müssen geschützt werden.

Die Reichweite von RFID beträgt weniger als einen Meter. Aufgrund dieser begrenzten Reichweite ist die physische Zugangsbeschränkung eine gültige Sicherheitsmaßnahme für RFID. So kann der Besitzer einer RFID-Karte die Informationen auf seiner RFID-Karte schützen, indem er den Zugang zu seiner RFID-Karte einschränkt.

Meistens werden die Informationen nur von der RFID-Karte gelesen. Manchmal werden auch Informationen auf die RFID-Karte geschrieben. In beiden Fällen wird nur eine begrenzte Menge an Daten übertragen. Es wird kein Kommunikationsprotokoll erstellt, das den Zugang zu Netzwerkdiensten ermöglicht. Aus diesem Grund sind für RFID keine zusätzlichen Sicherheitsmaßnahmen wie Authentifizierung und Verschlüsselung erforderlich.

WLAN

Die Reichweite von WLAN beträgt mehr als 10 Meter. Daher ist eine physikalische Zugangsbeschränkung für WLAN nicht möglich. Für KEBA IACS-Komponenten werden WLAN-Schnittstellen als Schnittstellen zum Automatisations-Netzwerk betrachtet. Daher sind die Anforderungen an die Sicherheit von Kommunikationsprotokollen auf im WLAN identisch mit den An-

© KEBA 2021

forderungen an Kommunikationsprotokolle im Automatisations-Netzwerk. Für die Kommunikation über das WLAN wird eine Authentifizierung und Verschlüsselung empfohlen.

Unabhängig davon, welche Kommunikationsprotokolle verwendet werden, sollte das WLAN selbst authentifiziert und verschlüsselt sein. Es liegt in der Verantwortung des Betreibers des Zugangspunkts, der häufig der Eigentümer der Anlage ist, das erforderliche Sicherheitsniveau zu konfigurieren.

WLAN-Zugangspunkt für KeControl

KeControl-Geräte sind in der Lage, als Zugangspunkt zu arbeiten, wenn die installierte Software diese Funktion unterstützt. Um den Zugangspunkt zu aktivieren, genügt es, einen unterstützten USB-WLAN-Adapter an einen USB-Port anzuschließen. Der Zugangspunkt startet automatisch mit einem WPA-geschützten WLAN. Die SSID ist die MAC-Adresse des verwendeten USB-WLAN-Adapters und die Passphrase ist die Seriennummer des KeControl-Gerätes.

Ähnlich wie bei normalen WLAN-Schnittstellen wird auch das WLAN dieses Zugangspunkts als Automatisations-Netzwerk betrachtet. Daher ist das erforderliche Sicherheitsniveau für Kommunikationsprotokolle im WLAN identisch mit den Anforderungen für Kommunikationsprotokolle im Automatisations-Netzwerk. Für die Kommunikation über das WLAN wird Authentifizierung und Verschlüsselung empfohlen.

Mit der Firewall können die Protokolle im WLAN auf sichere Protokolle beschränkt werden. Auf diese Weise ist die Sicherheit der Kommunikation unabhängig von der WLAN-Sicherheit. Dies ist eine wichtige Eigenschaft, da die WPA-Passphrase nicht zufällig ist. Daher wird empfohlen, dass die Firewall die Kommunikation im WLAN auf sichere Protokolle beschränkt, wenn die WLAN- Zugangspunkt-Funktion verwendet wird.

Drahtloses KeTop-System

Wird ein drahtloses KeTop-System, bestehend aus einem Handbediengerät und einer Basisstation, als Kabelersatz verwendet, wird die Verbindung durch den Pairing-Prozess authentifiziert (zusammengehalten) und verschlüsselt. In einem anderen Anwendungsfall sind alle beschriebenen Netzwerkvorkehrungen zu beachten.

1.3.2.9 Physische Schnittstellen

KEBA-IACS-Komponenten haben zusätzlich zu den bereits besschriebenen Netzwerkdiensten physikalische Schnittstellen. Die spezifischen Sicherheitseigenschaften dieser physikalischen Schnittstellen müssen bekannt sein, um entscheiden zu können, ob eine physikalische Schnittstelle verwendet werden soll und wie sie konfiguriert wird, um das erforderliche Sicherheitsniveau zu gewährleisten.

KEBA © KEBA 2021

Anzeige- und Bedienelemente

Benutzerschnittstellen wie Displays mit Tasten, Reglern, werden zunächst durch den geografischen Standort authentifiziert. Für den Zugriff auf die grafische Benutzeroberfläche und die Schaltflächen eines KeTop-Geräts ist der Zugang zu den Produktionsräumen erforderlich. Außerdem ist der Zugang zum Schaltschrank erforderlich, um auf das Display und die Tasten von KeControl- und KeDrive-Geräten zuzugreifen.

In den Produktionsräumen zugängliche Visualisierungsgeräte wie KeTop erfordern oft eine zusätzliche Authentifizierung, um mehr oder den vollen Funktionsumfang zu ermöglichen. Für diese zusätzliche Authentifizierung werden üblicherweise Passwörter und Schlüsselkarten verwendet. Basierend auf dieser Authentifizierung werden die Rollen und Benutzer auf visualisierungsspezifische Benutzerrechte für die Visualisierung geprüft. Basierend auf den zugewiesenen Rechten auf Benutzerebene erlaubt die Visualisierungsanwendung den Zugriff auf bestimmte Funktionen oder nicht.

Visualisierungsanwendungen sind immer bildschirmfüllend. Sie erlauben keinen Zugriff auf den Desktop des Betriebssystems, um beliebige Anwendungen zu starten und zu beenden. Wenn mehrere Visualisierungsanwendungen unterstützt werden, wird ein Kiosk-Desktop verwendet. Ein Kiosk-Desktop erlaubt nur die Ausführung ausgewählter Anwendungen - diese werden vom Administrator oder Anwendungsentwickler auf dem Gerät installiert und konfiguriert, nicht vom normalen Benutzer.

Handelt es sich bei der Visualisierung um eine auf einer Webschnittstelle basierende Anwendung, dann reichen Rechte auf Benutzerebene nicht aus. Die Weboberfläche prüft, ob andere Rechte als die Benutzerrechte vorhanden sind und verweigert den Zugriff, wenn die erforderlichen Rechte fehlen. Daher muss die Visualisierungsanwendung den Benutzer auch gegenüber der Weboberfläche authentifizieren, um die Nutzung von Funktionen zu ermöglichen, die die Weboberfläche erfordern.

Die Sicherheitseigenschaften für Anzeigen und Bedienelemente sind:

Dienst	Anzeige- und Bedienelemente
Authentifizierung der Anwendung	Geografischer Standort
Benutzerauthentifizierung	Geografischer Standort, wahlweise Passwort oder Schlüsselkarte
Zugangsrechte	Definiert nach Anwendung, KEBA-Benutzerverwaltung für webbasierte Anwendung

USB-Schnittstellen

USB-Schnittstellen werden zumindest durch den geografischen Standort authentifiziert. Ein Benutzer muss in der Lage sein, ein Kabel oder ein Gerät an den USB-Anschluss anzuschließen. USB-Schnittstellen bieten eine breite Palette von Funktionen. Diese Funktionen können wie folgt gruppiert werden:

© KEBA 2021

- **USB-Host-Schnittstelle**: Der USB-Anschluss wird verwendet, um USB-Geräte wie USB-Sticks anzuschließen und von Anwendungen, die auf einem Betriebssystem laufen, auf sie zuzugreifen. Die tatsächlich zugänglichen Funktionen sind sehr unterschiedlich; so kann ein USB-Stick z. B. zur Bereitstellung von Dateien oder zur automatischen Installation von Software verwendet werden.
- **USB-Gerät**: Der USB-Anschluss ermöglicht den Zugriff auf ein genau definiertes USB-Gerät. Dies ist das Gegenteil zur USB-Host-Schnittstelle. Das USB-Gerät wird an eine USB-Host-Schnittstelle angeschlossen. Die KeDrive-USB-Netzwerkschnittstelle ist ein Beispiel für ein USB-Gerät. Sie bietet eine USB-basierte Netzwerkschnittstelle zu einem Service-Laptop.
- **USB-Boot**: Das Betriebssystem auf dem USB-Stick wird direkt durch das BIOS oder den Bootloader gebootet. Dies ist eine spezielle Funktion einer USB-Host-Schnittstelle.
- **USB-BIOS-Tastatur**: Der Zugriff auf das BIOS-Menü erfolgt über eine über USB angeschlossene Tastatur.

Diese Liste zeigt, dass USB für verschiedene Funktionen verwendet wird. Die Benutzerfreundlichkeit von USB erleichtert seine breite Anwendung.

Einige der über USB verfügbaren Funktionen ermöglichen einen starken Zugriff auf das Gerät. Daher wird empfohlen, die USB-Anschlüsse in einem Schrank unterzubringen, der ein hohes Maß an physischem Zugangsschutz gewährleistet. Nur wenn die geforderte Sicherheitsstufe ausreichend niedrig und der physische Zugriffsschutz auf die Werkshalle hoch genug ist, können USB-Anschlüsse direkt in der Werkshalle zugänglich gemacht werden.

1.3.2.10 Visualisierungs-Frameworks

KEBA bietet Visualisierungsframeworks wie z.B. KeView Style und KeView Trend zur Erstellung von Visualisierungen und fertige Visualisierungen wie z.B. TeachView. Die Grenze zwischen Frameworks und Visualisierungen ist fließend. Visualisierungs-Frameworks können gebrauchsfertige Masken und Dialoge bereitstellen. Gebrauchsfertige Visualisierungen können mit Parametern gesteuert und mit eigenem Code erweitert werden. Für beide, Frameworks und Visualisierungen, sind die folgenden Sicherheitsregeln zu beachten:

- **Sicherer Tunnel**: Wenn die Visualisierungsanwendung außerhalb des Maschinen-Netzwerkes läuft und Dienste ohne Authentifizierung und Verschlüsselung zur Kommunikation mit der Steuerung nutzt, muss die Kommunikation mit einem sicheren Tunnel gesichert werden. Dies ist bei allen Visualisierungsanwendungen der Fall, die nicht auf Web-Interfaces basieren. Als sicherer Tunnel kann OpenVPN verwendet werden. Läuft die Visualisierungsanwendung direkt auf der Steuerung oder auf einem Handheld-Terminal innerhalb des Maschinen-Netzwerkes, so ist ein sicherer Tunnel für die Kommunikation nicht erforderlich.
- **Web-Ressourcen**: Wenn die Visualisierung browserbasiert ist, muss HTTPS verwendet werden und alle von der Webanwendung verwendeten Ressourcen müssen innerhalb des Maschinen-Netzwerkes gehostet

KEBA © KEBA 2021

werden. Es dürfen keine Skripte, Bilder, Stylesheets, Schriftarten, REST-APIs, WebSocket-APIs, … im Automatisations-Netzwerk, im IT-Netzwerk oder gar im Internet gehostet werden. Dies ist notwendig, um die Bedrohung durch böswillige Eingaben in den Browser zu beseitigen, was die häufigste Sicherheitslücke bei Browsern darstellt. Dazu gehört auch das Surfen im Internet oder auf anderen nicht vertrauenswürdigen Websites. Die KEBA-Visualisierungssoftware, die einen Browser enthält, läuft im Kioskmodus, um zu verhindern, dass der Benutzer auf beliebige Websites gelangt. Das Surfen auf nicht vertrauenswürdigen Websites wie dem Internet ist für jede browserbasierte Visualisierungssoftware tabu.

1.3.2.11 Tools

Die KEBA-Tools sind in der Lage, über sichere Protokolle mit den KEBA-Geräten zu kommunizieren. Es gibt zwei Varianten der sicheren Kommunikation. Die erste Variante ist die Verwendung von Protokollen, die von vornherein sicher sind. Die zweite Variante ist die Verwendung von OpenVPN zum Tunneln von unsicheren Protokollen zwischen Werkzeug-PC und KEBA-Gerät.

Um sicherzustellen, dass im Automatisations-Netzwerk nur sichere Protokolle für die Werkzeugkommunikation verwendet werden, muss die Firewall der KEBA-Geräte so konfiguriert werden, dass nur sichere Protokolle zugelassen werden. Auf diese Weise können Protokolle mit schwacher oder fehlender Sicherheit nicht versehentlich verwendet werden.

1.3.2.12 Software-Updates

Software muss von Zeit zu Zeit auf neue Versionen aktualisiert werden. Es gibt viele Gründe für ein Software-Update:

- **Sicherheitsproblem behoben**: Ein Sicherheitsfehler, der für die eigentliche Anwendung der Software relevant ist, wurde in der neuen Version behoben.
- **Funktionsfehler behoben**: Ein Funktionsfehler, der sich negativ auf den Betrieb der Software auswirkt, wurde in der neuen Version behoben.
- **Zusätzliche Funktion**: Die neue Version enthält eine neue Funktion, die von den Benutzern benötigt wird oder die erforderlich ist, um andere von dieser Funktion abhängige Erweiterungen zu aktivieren.
- **Verlängerter Supportzeitraum**: Das Ende des Supportzeitraums der aktuellen Version ist nahe und die Software soll auch in Zukunft weiter genutzt werden.

Aktualisierungen können bei Bedarf oder in regelmäßigen Abständen vorgenommen werden. Um die Sicherheit der verwendeten Software zu gewährleisten, werden regelmäßige Updates empfohlen.

KEBA verwendet modernste Entwicklungsprozesse, um das Risiko von Sicherheits- und Funktionsfehlern zu minimieren. Trotzdem können Bugs nicht vollständig verhindert werden. Diese verbleibenden Fehler können potenziell ausgenutzt werden, um die Sicherheit eines Gerätes zu brechen, z.B. um Aktionen ohne die notwendige Authentifizierung auszuführen. Software-Up-

© KEBA 2021

dates sind der weit verbreitete und anerkannte Weg, um Bugs in der Praxis zu beheben. Daher sind Software-Updates für jede KEBA-IACS-Komponente möglich.

1.3.3 Defense in Depth

"Defense in Depth" ist eine Sicherheitsstrategie, die mehrere Sicherheitsebenen verwendet, um einzelne Sicherheitsprobleme oder Fehler zu tolerieren. Einzelne Sicherheitslücken, wie Softwareschwachstellen, werden auftreten. Folglich können nur zusätzliche Sicherheitsebenen das Sicherheitsrisiko verringern, wenn eine Sicherheitslücke vorhanden ist. Auch die IEC 62443 definiert als Sicherheitsstrategie "Defense in Depth". Es wird daher davon ausgegangen, dass "Defense in Depth" vom Anlagenbesitzer, dem Systemintegrator und dem Maschinenbauer implementiert wird. KEBA-Produkte unterstützen verschiedene Sicherheitsebenen, die die Umsetzung der "Defense in Depth"-Strategie erleichtern.

Es gibt verschiedene Möglichkeiten zur Implementierung von Sicherheitsebenen. Diese Optionen lassen sich in physische und logische Sicherheitsebenen unterteilen. Physische Sicherheitsebenen werden an verschiedenen Stellen implementiert, meist innerhalb der Umgebung und auf der Ebene des IACS. Beispiele hierfür sind Tore auf dem Gelände und in Gebäuden, die nur mit gültigen Schlüsselkarten passiert werden können. Auch Türschlösser für Schränke sind physische Sicherheitsmaßnahmen. Die logischen Sicherheitsmaßnahmen sind vielfältiger und können nach Standort gruppiert werden:

- **Umgebung:** In der Umgebung werden logische Sicherheitsschichten in Form von Firewalls implementiert. Sie bilden Zonen, die die Ausbreitung von Sicherheitsbedrohungen verhindern können.
- **IACS:** Auf der Ebene der industriellen Automatisierungs- und Kontrollsysteme werden Sicherheitsebenen in Form von Authentifizierung, Verschlüsselung und geringstmöglicher Privilegierung verwendet. Auch Firewalls sind für IACS relevant.
- **IACS-Komponente:** Ähnlich wie ein IACS implementieren auch seine Komponenten Sicherheit in Form von Identifizierung, Authentifizierung, Verschlüsselung, geringstem Privileg und Auditing. Zusätzlich werden Integritätsprüfungen als Sicherheitsebene verwendet.

1.3.4 Geschützte Umgebung

Die Umgebung für den Betrieb eines IACS hat großen Einfluss auf das erreichbare Sicherheitsniveau. Wenn z.B. jeder physischen Zugang zum Schaltschrank einer Anlage hat, kann ein hohes Sicherheitsniveau nicht erreicht werden. Die Verkabelung könnte leicht manipuliert werden, was schwerwiegende Folgen hätte. Daher ist es eine gängige Maßnahme, den physischen Zugang nur einem begrenzten Personenkreis zu gestatten, um ein Mindestmaß an Sicherheit zu gewährleisten. Welche Maßnahmen ergriffen werden, hängt von der Sicherheitsstufe ab, die erreicht werden soll. Diese Zielsicherheitsstufe wird vom Eigentümer des IACS festgelegt.

KEBA © KEBA 2021

Eine einzelne IACS-Komponente kann kein bestimmtes Sicherheitsniveau für das gesamte IACS garantieren. Die Bedrohungen und die notwendigen Maßnahmen zu ihrer Abwehr hängen stark von der Anwendung ab und müssen oft auf Systemebene implementiert werden. Letztendlich wird ein IACS immer in einer geschützten Umgebung betrieben, da die Bedrohungen und Risiken in einer beliebigen Umgebung nicht abgemildert werden können. Daher ist eine geschützte Umgebung eine vernünftige Annahme und kann als Voraussetzung für den sicheren Betrieb von IACS-Komponenten festgelegt werden

Die Sicherheitsmaßnahmen, die innerhalb dieser geschützten Umgebung eingerichtet werden, leiten sich aus dem erforderlichen Sicherheitsniveau des Anlagenbesitzers ab. Jeder Anlageneigentümer muss das richtige Gleichgewicht zwischen ausreichenden Sicherheitsmaßnahmen finden, die das geforderte Sicherheitsniveau herstellen und nicht zu vielen Sicherheitsmaßnahmen, die die Kosten (Betrieb, Wartung, …) erhöhen.

Die folgende Liste gibt einen Überblick über gängige Sicherheitsmaßnahmen:

- **Physische Zugangskontrolle zu den Produktionsräumen:** Nur Personen mit Zugangsberechtigung können die Produktionsräume betreten.
- **Physische Zugangskontrolle zum Schaltschrank der Maschine:** Nur Personen, die im Schrank arbeiten müssen, können den Schrank öffnen.
- **Passwort-Richtlinien** Das Passwort muss sicher sein und als persönliches Geheimnis aufbewahrt werden.
- **Isoliertes Netzwerk für die Produktionsräume:** Das Netzwerk, das die Maschinen in der Fertigung verbindet (Automatisierungsnetz), muss von allen anderen Netzen wie dem IT-Netz durch eine Firewall isoliert sein. Ein IACS darf niemals in offenen Netzen oder im Internet betrieben werden. Dadurch wird auch die Zuverlässigkeit des Netzes erhöht.
- **Sichere Kommunikation:** Verwendung von authentifizierten und verschlüsselten Kommunikationsmechanismen wie OPC UA, HTTPS, VPN oder SSH zur Kommunikation mit dem IACS.
- **Anzahl von offengelegten Schnittstellen minimieren:** Keine Schnittstellen von IACS-Komponenten wie USB- oder Netzwerkanschlüsse in den Produktionsräumen zur Verfügung stellen. Die einzige Ausnahme sind USB-Anschlüsse von KeControl- und KeTop-Geräten, die für diesen Anwendungsfall konzipiert sind.
- **IT-Sicherheitsmaßnahmen für IT-Geräte:** Verwendung modernster IT-Sicherheitsmaßnahmen für IT-Geräte, unabhängig davon, ob sie sich innerhalb des IT-Netzwerks oder des Netzwerks auf in den Produktionsräumen (Automatisierungsnetz) befinden. Insbesondere IT-Geräte, die eine Verbindung zu IACS-Komponenten herstellen können, müssen berücksichtigt werden, da ihr Sicherheitsniveau direkten Einfluss auf das Sicherheitsniveau der IACS-Komponenten hat. Ein Beispiel für eine IT-Sicherheitsmaßnahme ist der Einsatz von Virenscannern auf Desktop-PCs, die in der Produktion eingesetzt werden. Es ist zu beachten, dass für IACS-Komponenten IT-Sicherheitsmaßnahmen wie Virenscanner oft nicht geeignet sind. Insbesondere Steuerungen können nicht wie IT-Geräte behandelt werden.

© KEBA 2021

- **Wiederherstellung:** Im Falle eines Sicherheitsvorfalls ist das Ziel, alle Systeme wieder in den Normalzustand zu versetzen. Daher ist eine Wiederherstellungsstrategie erforderlich. Backups sind oft ein wichtiger Teil der Wiederherstellungsstrategie. Es sind Tests erforderlich, um sicherzustellen, dass die Wiederherstellungsverfahren im Bedarfsfall tatsächlich funktionieren.

Die tatsächliche Auswahl der Sicherheitsmaßnahmen und die Berechnung des insgesamt erreichten Sicherheitsniveaus erfolgt durch den Eigentümer der Anlage.

1.3.5 Netzwerkarchitektur

Es ist sehr üblich, dass Maschinen innerhalb der Produktionsräume kommunizieren. Sie kommunizieren z.B. mit SCADA-Systemen während der Produktion und mit Diagnosewerkzeugen. Dieses Netzwerk in den Produktionsräumen ist das Automationsnetzwerk. Wie bereits erwähnt, muss dieses Automationsnetzwerk aus Gründen der Sicherheit und Zuverlässigkeit von anderen Netzen isoliert werden. Die Kommunikationsschnittstelle der Maschine zum Automationsnetzwerk bildet eine Grenze zwischen der Maschine und dem Automationsnetzwerk. Die gesamte Kommunikation über diese Schnittstelle ist hochgradig sicherheitsrelevant. Daher müssen alle auf dieser Schnittstelle verwendeten Protokolle bekannt sein und unter Sicherheitsaspekten ausgewählt werden.

Die Kommunikationsschnittstelle zwischen der Maschine und dem Automations-Netzwerk ist oft mehr als nur eine Grenze zwischen der Maschine und dem Fertigungsbereich. Maschinen beinhalten oft ein internes Netzwerk zwischen ihren IACS-Komponenten. In diesem Fall ist die Kommunikationsschnittstelle eine Grenze zwischen zwei Netzwerken, dem internen Maschinen-Netzwerk und dem externen Automations-Netzwerk. Aber unabhängig davon, ob die Maschine aus einer einzelnen SPS oder mehreren IACS-Komponenten besteht, ist die Kommunikation über diese Schnittstelle in beiden Fällen höchst sicherheitsrelevant.

Eine Maschine ohne internes Maschinen-Netzwerk ist ein Sonderfall, der hier nicht gesondert betrachtet werden muss. Er stellt nur das absolute Minimum eines internen Maschinen-Netzwerkes dar. Eine solche Maschine birgt keine zusätzlichen Sicherheitsrisiken im Vergleich zu einer Maschine mit einem internen Maschinen-Netzwerk. Sobald eine Feldbuskommunikation genutzt wird, wird ein internes Maschinen-Netzwerk aufgebaut. Eine Maschine ohne internes Maschinen-Netzwerk ist daher ein sehr seltener Fall. Insgesamt kann davon ausgegangen werden, dass dieser Sonderfall keiner weiteren Betrachtung bedarf und in die Betrachtung über Maschinen mit internem Netzwerk einbezogen wird.

Benennung der Netzwerke

Für die Netzwerke auf beiden Seiten der Grenze sind auf dem IACS-Markt mehrere Bezeichnungen gebräuchlich. Ohne einen Anspruch auf Vollständigkeit zu erheben, könnten die folgenden Bezeichnungen für das Netzwerk in den Produktionsräumen zwischen mehreren Maschinen verwendet werden:

KEBA © KEBA 2021

- **Automations-Netzwerk**
- Netzwerk der Produktionsstätten
- Steuerungsnetzwerk
- Produktionsraum-Netzwerk
- Produktionsnetzwerk
- Werksnetz
- Externes Netzwerk (außerhalb der Maschine)
- Internes Netzwerk (innerhalb der Produktionsräume)

Wiederum ohne Anspruch auf Vollständigkeit könnten für das interne Netzwerk der Maschine die folgenden Namen verwendet werden:

- **Maschinen-Netzwerk**
- Internes Netzwerk

In diesem Dokument werden die Bezeichnungen "Automations-Netzwerk" und "Maschinen-Netzwerk" verwendet.

"Boundary protection device"

Die Verbindung zwischen dem Automations-Netzwerk und dem Maschinen-Netzwerk wird durch ein Gerät hergestellt, das an beide Netze angeschlossen ist. Dieses Gerät wird in diesem Dokument als "Boundary protection device" bezeichnet. Die Rolle des "Boundary protection device" kann von jedem Gerät ausgefüllt werden, das in der Lage ist, in beiden Netzwerken zu arbeiten. Es ist zu beachten, dass das Maschinen-Netzwerk ein Feldbus, ein IP-basiertes Netzwerk oder eine Kombination aus beiden Netzwerkarten sein kann.

Folgend werden Beispiele für "Boundary protection devices" zum besseren Verständnis aufgelistet. Die Beispiele können für komplexere Systeme kombiniert werden:

- SPS: Ethernet-Schnittstelle für Automatisations-Netzwerk und EtherCAT-Schnittstelle für Maschinen-Netzwerk mit IOs und Antrieben.
- Aktives Panel: Ethernet-Schnittstelle für Automatisations-Netzwerk und Ethernet-Schnittstelle für Maschinen-Netzwerk mit SPS.
- Gateway: Generisches Gateway-Gerät mit Ethernet-Schnittstelle für Automatisations-Netzwerk und Ethernet-Schnittstelle für Maschinen-Netzwerk mit SPS.

Für das Automatisations-Netzwerk ist in der Regel ein höheres Sicherheitsniveau erforderlich als für das Maschinen-Netzwerk, da dieses stärker von Sicherheitsbedrohungen betroffen ist. Da das "Boundary protection device" Teil beider Netzwerke ist, sind die Sicherheitsanforderungen für das "Boundary protection device" höher als für andere Geräte innerhalb des Maschinen-Netzwerks. Das "Boundary protection device" muss das für das Automatisations-Netzwerk erforderliche Sicherheitsniveau erreichen. Daher wird die Sicherheit der "Boundary protection devices" gesondert berücksichtigt.

© KEBA 2021

Segmentierung des Netzwerks

Das "Boundary protection device" erzwingt eine Segmentierung zwischen Automatisations-Netzwerk und Maschinen-Netzwerk. Die Netzwerksegmentierung bietet Vorteile für Sicherheit, Zuverlässigkeit und Wartung. Im Hinblick auf die Sicherheit werden die Exposition und die Ausbreitung des Maschinen-Netzwerkes auf das Automatisations-Netzwerk reduziert. Dienste können nur für das Maschinen-Netzwerk bereitgestellt werden. Die IACS-Komponenten innerhalb des Maschinen-Netzwerkes können nicht auf beliebige Weise auf das Automatisations-Netzwerk zugreifen, da das "Boundary protection device" diesen Zugriff begrenzt.

Die Zuverlässigkeit wird verbessert, da der Datenverkehr innerhalb der Netzwerke reduziert wird. Der lokale Datenverkehr innerhalb des Automatisations-Netzwerkes bleibt innerhalb des Automatisations-Netzwerkes und beeinträchtigt das Maschinen-Netzwerk nicht. Dies gilt umgekehrt auch für das Maschinen-Netzwerk.

Auch Service und Wartung sind einfacher, wenn die Maschine als ein einziges Gerät innerhalb des Automatisations-Netzwerkes erscheint. Eine für das Automatisations-Netzwerk spezifische IP-Adresse muss nur dem "Boundary protection device" der Maschine zugewiesen werden. Die IACS-Komponenten innerhalb des IP-basierten Maschinen-Netzwerkes verwenden private IP-Adressen, die nicht mit IP-Adressen des Automatisations-Netzwerkes in Konflikt geraten können. Andernfalls würden alle IACS-Komponenten innerhalb des IP-basierten Maschinen-Netzwerkes Automatisations-Netzwerk-spezifische IP-Adressen benötigen. Dies führt zu erhöhtem Aufwand und Komplexität bei der Inbetriebnahme der Maschine.

Sobald das "Boundary protection device" als Router/Gateway fungiert, werden diese Vorteile der Netzsegmentierung erheblich eingeschränkt. Am wichtigsten ist in diesem Fall, dass nun eine direkte Kommunikation zwischen den Segmenten möglich ist, was sonst nicht der Fall ist. Wenn das "Boundary protection device" als Switch fungiert, dann gibt es keine Netzsegmentierung und keine der Vorteile sind gültig.

Die Netzwerksegmentierung ermöglicht die Realisierung von Zonen und Durchleitungen, wie sie für die Bedrohungs- und Risikobewertung des IACS empfohlen werden.

Topologie des Netzwerks

Die Netzwerktopologie ist die Anordnung der Elemente des Kommunikationsnetzes. Die Anordnung und die verwendeten Elemente unterscheiden sich in zahlreichen Details bei jedem Netz. Aus der Übersichtsperspektive werden die Unterschiede kleiner und gemeinsame Eigenschaften werden sichtbar. Daher ist es möglich, eine Referenz-Netzwerktopologie zu definieren, die auf die Mehrzahl der bestehenden Kommunikationsnetze passt.

Die Referenz-Netztopologie, die für ein IACS mit KEBA-Produkten angenommen wird, ist in folgender Abbildung dargestellt.

KEBA © KEBA 2021

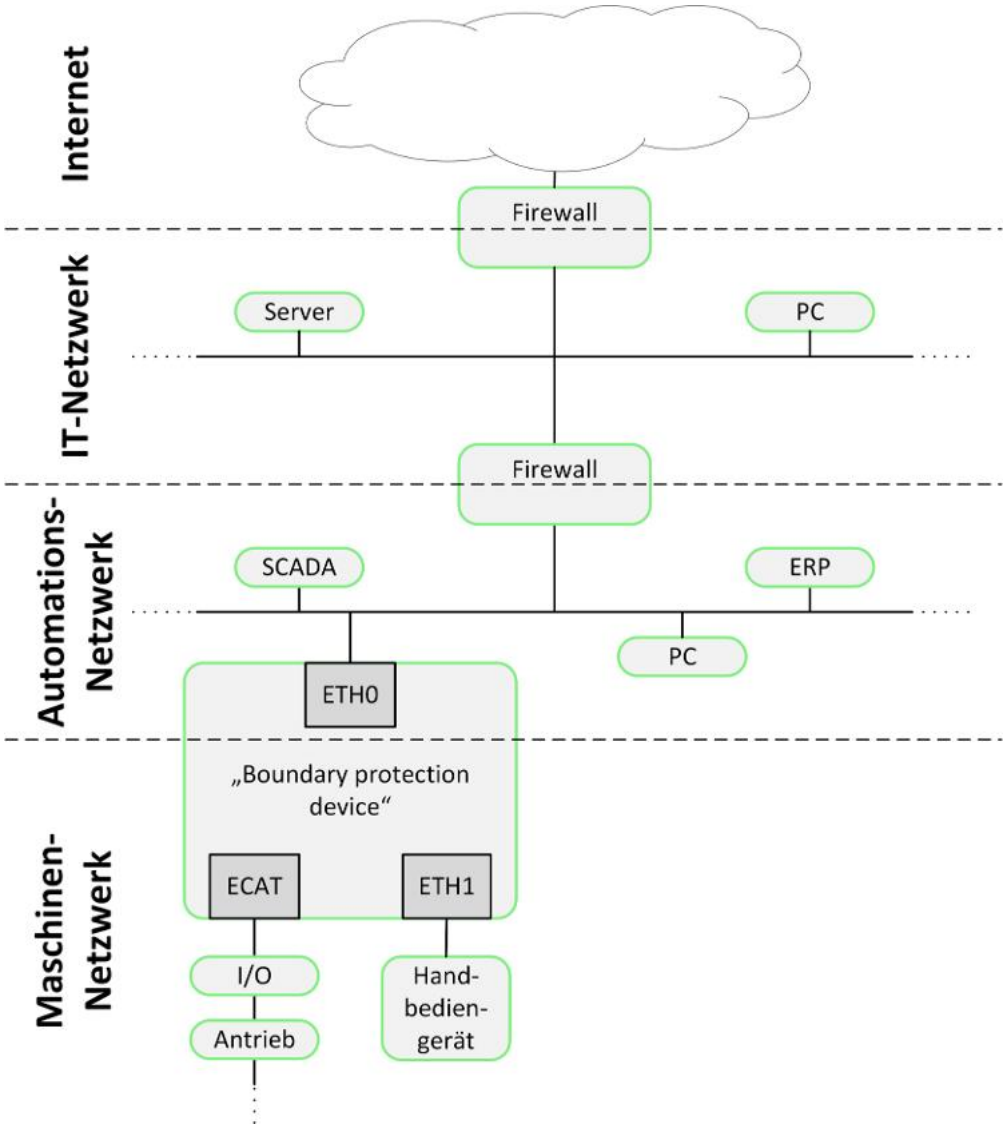


Abb. 1-1: Referenz-Netzwerktopologie

Das Internet ist das globale Netzwerk, das Büros, Fabriken, Geräte, … rund um die Welt verbindet. Das Internet ist nicht vertrauenswürdig . Das Internet bietet zwar viele Vorteile, aber seine Sicherheit entwickelt sich immer weiter, mit ständigen Herausforderungen wie Datenschutzverletzungen, Fehlinformationen und dem Bedarf an stärkeren Verschlüsselungs- und Authentifizierungsmaßnahmen, weshalb das Internet kein vertrauenswürdiges Netzwerk ist.

Das IT-Netzwerk ist mit dem Internet verbunden. Es handelt sich um ein separates Netzsegment, das durch eine Firewall geschützt ist, um die vom Eigentümer der Anlage geforderte Sicherheitsstufe zu erreichen. Die Abbildung zeigt ein einfaches IT-Netz. Oftmals bestehen IT-Netze aus mehreren Netzsegmenten, z. B. einer separaten Zone für Server.

Das IACS befindet sich nicht innerhalb des IT-Netzwerkes. Das IACS wird innerhalb des Automatisations-Netzwerkes realisiert, das wiederum ein separates, vom IT-Netzwerk durch eine Firewall getrenntes Netzsegment dar-

© KEBA 2021

stellt. Innerhalb des Automatisations-Netzwerkes gibt es ein oder mehrere IACS. Diese IACS bestehen aus Maschinen, Geräten oder anderen Anlagen. Auch eine einzelne Maschine kann ein IACS sein.

Das interne Netzwerk einer Maschine wird als Maschinen-Netzwerk bezeichnet. Dieses Netzwerk ist mit dem Automatisations-Netzwerk durch ein "Boundary protection device" verbunden, um diese Netzwerke voneinander zu trennen. Mehrere Maschinen-Netzwerke können an ein einziges Automatisations-Netzwerk angeschlossen werden.

Netzwerkdienste

Maschinen können Dienste für das Automatisations-Netzwerk bereitstellen. Diese Dienste können während des Betriebs oder bei Bedarf, z.B. zur Diagnose, genutzt werden. Die Dienste werden vom "Boundary protection device" bereitgestellt, da die Netzwerksegmentierung erzwingt, dass nur das "Boundary protection device" Zugang zum Automatisations-Netzwerk hat. Andere IACS-Komponenten innerhalb des Maschinen-Netzwerkes können keine Dienste direkt für das Automatisations-Netzwerk bereitstellen. Jeder Dienst erhöht das Sicherheitsrisiko eines Geräts und natürlich auch des "Boundary protection device". Daher sind die bereitgestellten Dienste auf das notwendige Minimum zu reduzieren.

Wenn ein Dienst einer IACS-Komponente innerhalb des Maschinen-Netzwerkes auf dem Automatisations-Netzwerk bereitgestellt werden soll, dann muss das "Boundary protection device" diesen Dienst weiterleiten. Diese Weiterleitung kann generisch auf IP-Ebene (Schicht 3) oder protokollspezifisch erfolgen. Die generische Weiterleitung auf IP-Ebene führt zu einer hohen Exposition der IACS-Komponente gegenüber dem Automatisations-Netzwerk. Eine protokollspezifische Weiterleitung wie z.B. die HTTP-Weiterleitung führt zu einer geringeren Exposition im Vergleich zur generischen Weiterleitung, kann aber nicht auf jedes Protokoll angewendet werden.

Das "Boundary protection device" kann Dienste für das Automatisations-Netzwerk und das Maschinen-Netzwerk bereitstellen, da es mit beiden Netzen verbunden ist. Standardmäßig werden die Dienste für alle angeschlossenen Netze bereitgestellt. Aufgrund der vom "Boundary protection device" vorgenommenen Netzwerksegmentierung sind die Sicherheitsüberlegungen für beide Netzwerke in der Regel unterschiedlich. So ist ein Dienst, der für ein Netzwerk sicher genug ist, nicht unbedingt auch für das andere Netzwerk sicher genug. Die Gefährdung des Automatisations-Netzwerkes ist höher als die des Maschinen-Netzwerkes. Daher kann ein Dienst für das Maschinen-Netzwerk sicher genug sein, aber nicht für das Automatisations-Netzwerk. Daher kann es ein Sicherheitsproblem darstellen, wenn jeder Dienst des "Boundary protection device" für das Automatisations-Netzwerk bereitgestellt wird. Die Lösung besteht darin, nur eine Teilmenge aller aktivierten Dienste des "Boundary protection device" für das Automatisations-Netzwerk bereitzustellen. Dies wird in der Regel durch eine Firewall auf dem "Boundary protection device" erreicht. Auch die Bindung von Diensten einzig an die Schnittstelle des Maschinen-Netzwerkes ist eine gültige Lösung.

KEBA © KEBA 2021

Ausgehende Netzwerkkommunikation

Neben den Netzwerkdiensten gibt es auch die abgehende Netzwerkkommunikation, die ebenfalls sicherheitsrelevant ist. Jede Netzwerkommunikation ist durch Abhören, Spoofing, Manipulationen usw. bedroht. Daher ist es ein allgemeiner Sicherheitsgrundsatz, die Netzwerkkommunikation auf das notwendige Minimum zu reduzieren. Wie bereits erwähnt, ist die Gefährdung des Automatisations-Netzwerkes höher als die des Maschinen-Netzwerkes. Daher ist es sinnvoll, der verwendeten Kommunikation im Automatisations-Netzwerk besondere Aufmerksamkeit zu schenken. Aufgrund der Netzwerksegmentierung kann nur das "Boundary protection device" im Automatisations-Netzwerk kommunizieren. Durch die Begrenzung der vom "Boundary protection device" initiierten Kommunikation im Automatisations-Netzwerk wird daher die gesamte von der Maschine initiierte Kommunikation im Automatisations-Netzwerk eingeschränkt

Netzwerkdienste können normalerweise durch die Konfiguration der IACS-Komponente aktiviert und deaktiviert werden. Ähnliche ausgehende Netzwerkkommunikation muss normalerweise durch Konfiguration aktiviert werden; z.B. ermöglicht die Konfiguration einer NTP-Server-IP-Adresse die Kommunikation mit diesem Server. Zusätzlich kann die ausgehende Netzwerkkommunikation durch Anwendungen ausgelöst werden. Dies kann entweder direkt oder indirekt geschehen. Eine Netzwerkkommunikation wird direkt durch Programmierung gegen eine Socket-API ausgelöst; z.B. die Linux POSIX Socket-API. Eine indirekte Auslösung erfolgt durch die Verwendung einer API-Funktion, die intern die Socket-API verwendet, z. B. durch die Verwendung einer FTP-Bibliothek.

1.3.6 Netzwerkeigenschaften

Die Netzwerke der Produktionsräume wie das Automatisations-Netzwerk und die Maschinen-Netzwerke ermöglichen eine kosteneffiziente Produktion und sind entscheidend für den wirtschaftlichen Erfolg. Verfügbarkeit und Integrität haben in der Regel eine höhere Priorität als Vertraulichkeit. Im Gegensatz dazu ist bei IT-Netzwerken die Vertraulichkeit in der Regel das wichtigste Ziel. Daher haben Produktionsnetzwerke im Vergleich zu IT-Netzwerkwerken andere Eigenschaften.

Netzwerke an Produktionsstandorten sind fast immer durch eine physische Zugangskontrolle geschützt. Nur befugte Personen können auf die Netzwerk-Hardware und Netzwerk-Ports zugreifen. Dieser Schutz ist in der Regel strenger als bei IT-Netzwerken, die sich in Büros und auch in Besprechungsräumen für Gäste befinden.

Automatisations-Netzwerk

Das Automatisations-Netzwerk ist das Netzwerk im Betrieb, das die Kommunikation von Maschinen, SCADA, Arbeitsstationen und anderen für den Betrieb erforderlichen Geräten ermöglicht. Für die Kommunikation im Automatisations-Netzwerk stehen sichere Protokolle wie OPC UA zur Verfügung. Die Verwendung von sicheren Protokollen erfordert die Verwaltung und Pflege von Schlüsseln. Individuelle Schlüssel, die regelmäßig gewechselt werden, bieten ein hohes Sicherheitsniveau. Die Schlüsselverwaltung erfordert einen

© KEBA 2021

kontinuierlichen Aufwand. Wenn die Schlüsselverwaltung fehlschlägt, sinkt das Sicherheitsniveau und im schlimmsten Fall wird die Produktion aufgrund einer fehlgeschlagenen Authentifizierung gestoppt. Daher ist eine Softwareunterstützung zur Vereinfachung der Schlüsselverwaltung erforderlich.

Neben sicheren Protokollen können auch andere Sicherheitsmaßnahmen eingesetzt werden, um ein für den Anlagenbesitzer zufriedenstellendes Sicherheitsniveau zu erreichen. Passwörter sind immer noch eine gültige Sicherheitsmaßnahme. Das Risiko des Abhörens von Passwörtern kann durch Einschränkung des Kommunikationsflusses innerhalb des Automatisations-Netzwerkes verringert werden. Auch IP-Bereichseinschränkungen verringern die Angriffsfläche von Protokollen.

Das Automatisations-Netzwerk ist ein separates Netz, das durch eine Firewall vom IT-Netzwerk getrennt ist. Dies ist notwendig, da die Anforderungen an die Verfügbarkeit und Reaktionsfähigkeit des Automatisations-Netzwerkes höher sind als die des IT-Netzwerkes. Außerdem wird durch diese Firewall auch die Sicherheit verbessert, da die Kommunikation auf bestimmte Protokolle und eventuell auch auf ausgewählte IP-Bereiche beschränkt wird.

Maschinen-Netzwerk

Das Maschinen-Netzwerk ist ein internes Netz der Maschine und sehr spezifisch für den jeweiligen Maschinentyp. Etablierte IT-Sicherheitsmaßnahmen wie Verschlüsselung und Authentifizierung können oft nicht überall im Maschinen-Netzwerk eingesetzt werden. Die Eigenschaften des Maschinen-Netzwerkes sind ähnlich wie die des Automatisations-Netzwerkes, aber die Anforderungen an Verfügbarkeit und Reaktionsfähigkeit sind höher.

Innerhalb des Maschinen-Netzwerks sind Feldbusse wie z.B. EtherCAT im Einsatz. Diese Feldbusse sind für eine robuste Echtzeitkommunikation ausgelegt. Die Vertraulichkeit der Kommunikation war kein Designziel. Die über Feldbusse kommunizierten Daten sind zu einem bestimmten Zeitpunkt gültig; z.B. die Position des Roboters. Außerdem erfordert die Interpretation dieser Daten tiefe Kenntnisse über die Maschine, und es können nur historische Daten rekonstruiert werden. Daher müssen diese Daten nicht vertraulich behandelt werden. Außerdem würde die für die Verschlüsselung der Echtzeitkommunikation erforderliche CPU-Leistung die Kosten der IACS-Komponenten erheblich erhöhen.

Die Verschlüsselung und Authentifizierung der Kommunikation erfordert eine Schlüsselverwaltung. Jedes IACS würde einen oder mehrere Schlüssel benötigen. Wie bereits erwähnt, erfordert diese Schlüsselverwaltung einen kontinuierlichen Aufwand. Wichtiger ist jedoch die Tatsache, dass IACS-Komponenten nicht mehr ohne weiteres ausgetauscht werden könnten. Der Austausch würde auch die Verteilung der Schlüssel auf die neue IACS-Komponente erfordern. Dies würde die Wartung und Instandhaltung erschweren und ist oft nicht durchführbar.

Innerhalb des Maschinen-Netzwerkes und insbesondere bei Feldbussen muss die Kommunikation Echtzeitanforderungen erfüllen. Selbst eine nur geringfügige Störung dieser Kommunikation kann zu Echtzeitverletzungen

KEBA © KEBA 2021

führen und würde einen Maschinenstopp zur Folge haben. Daher muss die Echtzeitkommunikation in jedem Fall isoliert werden, um das korrekte zeitliche Verhalten zu gewährleisten.

Zusammenfassend lässt sich sagen, dass die Kommunikation innerhalb des Maschinen-Netzwerkes nicht nur auf Protokollen mit Authentifizierung und Verschlüsselung basieren kann. Das "Boundary protection device" isoliert das Maschinen-Netzwerk vom Automatisations-Netzwerk und ermöglicht dedizierte Sicherheitsmaßnahmen für das Maschinen-Netzwerk. Die physische Zugangskontrolle für das Maschinen-Netzwerk ist in der Regel stärker eingeschränkt als für das Automatisations-Netzwerk. Außerdem ist es bewährte Praxis, dass eine direkte Kommunikation mit IACS-Komponenten innerhalb des Maschinen-Netzwerkes für Geräte, die nicht mit dem Maschinen-Netzwerk verbunden sind, nicht möglich ist. Das "Boundary protection device" fungiert nicht als Router und begrenzt die Kommunikation zum Maschinen-Netzwerk.

1.3.7 Fernzugriff

Für einige Anwendungsfälle ist es erforderlich, eine Verbindung zum Maschinen-Netzwerk herzustellen, ohne dass ein physischer Zugang zum Maschinen-Netzwerk besteht, z. B. für die Fernkonfiguration oder -diagnose mit Software-Tools. Diese Verbindungen werden bei Bedarf hergestellt und sind zeitlich begrenzt. Es gibt verschiedene Lösungen, um sichere Verbindungen über nicht vertrauenswürdige Netze herzustellen. Allen Lösungen ist gemeinsam, dass ein Terminaldienst auf einer IACS-Komponente innerhalb des Maschinen-Netzwerkes laufen muss. In der Regel läuft er auf dem "Boundary protection device". Auf dem Verbindungsgerät ist ein Softwaretool der gewählten Lösung erforderlich.

Wenn das "Boundary protection device" direkt über eine IP-Adresse erreichbar ist, können die weit verbreiteten VPN-Protokolle (Virtual Private Network) verwendet werden. Das VPN bietet eine authentifizierte und verschlüsselte Verbindung zum Maschinen-Netzwerk. Dienste, die innerhalb des Maschinen-Netzwerkes verfügbar sind, können auch über die VPN-Verbindung zur Verfügung gestellt werden. Mit VPN ist es möglich, auf Dienste von IACS-Komponenten zuzugreifen, einschließlich der "Boundary protection devices", die dem Maschinen-Netzwerk mehr Dienste zur Verfügung stellen kann als dem Automatisations-Netzwerk.

Oft ist das "Boundary protection device" nicht direkt über die IP-Adresse erreichbar. Dies ist der Fall, wenn sich die Maschine an einem Produktionsstandort eines anderen Unternehmens befindet. Ein Automatisations-Netzwerk ist fast immer ein privates Netz, das nicht über das Internet erreicht werden kann. Ein direkter Zugriff ist daher nur innerhalb des Netzes des Maschinenbesitzers möglich. Infolgedessen ist ein Agent notwendig, der die Verbindung vermittelt. Bei diesem Agenten handelt es sich um einen Internetdienst, da das Internet das einzige gemeinsame Netz ist, das für den Terminaldienst innerhalb des Maschinen-Netzwerkes und für das Softwaretool auf dem Anschlussgerät zur Verfügung steht. Sowohl der Terminaldienst als auch das Softwaretool verbinden sich mit dem Agenten. Diese Verbindungen müssen authentifiziert und verschlüsselt werden, da das Internet ein nicht vertrauenswürdiges Netz ist. Der Agent stellt eine Verbindung her, in-

© KEBA 2021

dem er die Kommunikation zwischen ihnen in beide Richtungen weiterleitet. Dieser Mechanismus ermöglicht Verbindungen, die mit VPN nicht möglich sind. Der Betrieb des Agenten verursacht Kosten für Datenverkehr, Speicherung und Wartung.

Beide Lösungen, VPN und die Verbindung über einen Agenten, ermöglichen einen vollständigen Zugriff auf das Maschinen-Netzwerk. Dies ist beabsichtigt, da dieser vollständige Zugang für Diagnose- und Wartungsaufgaben erforderlich ist. Allerdings birgt dies auch einige Sicherheitsrisiken, da die Dienste innerhalb der Maschinen-Netzwerke in der Regel weniger Sicherheitsmaßnahmen umsetzen als Dienste in anderen Netzen. Es muss also besonders darauf geachtet werden, dass diese Fernverbindungen die Angriffsfläche nicht vergrößern. So muss z.B. der Laptop, der für die Fernverbindung verwendet wird, mit IT-Sicherheitsmaßnahmen gesichert werden.

1.3.8 Referenz-IACS

Für die Diskussion der Sicherheitseigenschaften eines IACS und seiner Komponenten ist ein gemeinsames Verständnis der Topologie eines IACS erforderlich. Ein Referenz-IACS, das die tatsächlichen IACS-Topologien zusammenfasst, ist hilfreich.

Folgende Abbildung zeigt ein Referenz-IACS

KEBA © KEBA 2021

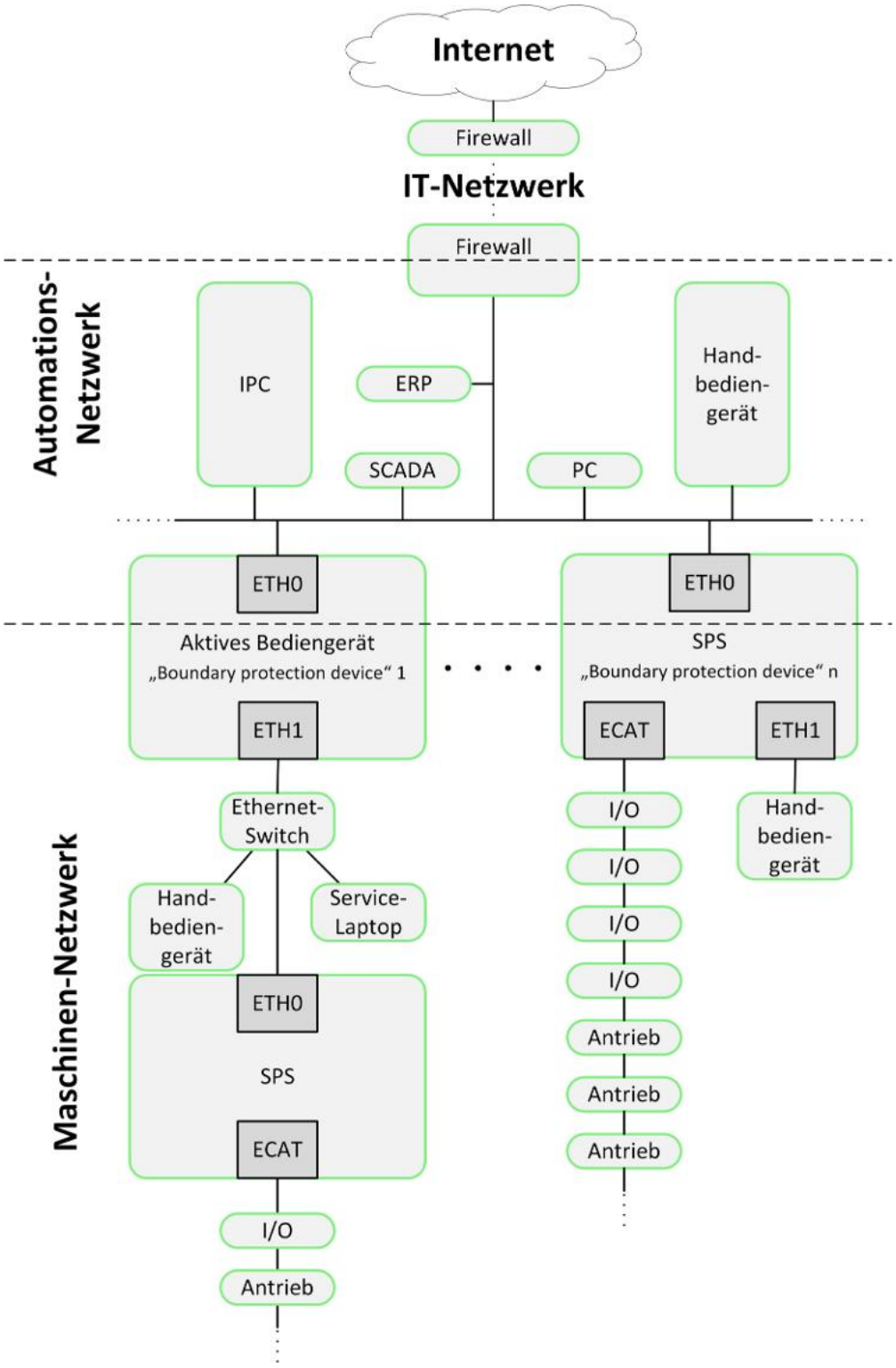


Abb. 1-2: Referenz-IACS

Das Rückgrat des IACS ist das Automatisations-Netzwerk. Das Automatisations-Netzwerk ist mit dem IT-Netzwerk und dem Internet verbunden, und alle Netze sind durch Firewalls voneinander getrennt. Innerhalb des Automatisations-Netzwerkes wird die hochrangige Funktionalität des IACS durch Ma-

© KEBA 2021

schinen und andere Geräte, die miteinander kommunizieren, hergestellt. Innerhalb des Automatisations-Netzwerkes können Geräte wie IPCs und Handheld-Terminals vorhanden sein. Maschinen und Anlagen mit einem internen Maschinen-Netzwerk sind über ein "Boundary protection device" mit dem Automatisations-Netzwerk verbunden. Es können ein oder mehrere "Boundary protection devices" vorhanden sein. Jedes "Boundary protection device" verbindet ein separates Maschinen-Netzwerk. Die Maschinen-Netzwerke sind nicht miteinander verbunden.

Maschinen-Netzwerke sind sehr unterschiedlich. Sie können Feldbusnetzwerke wie EtherCAT-Segmente mit Ein-/Ausgängen und Antrieben enthalten. Auch Ethernet-Netzwerke für Service-Laptops, Handheld-Terminals und andere Ethernet-basierte Geräte sind möglich. Auch Steuerungen und aktive Panels, die als "Boundary protection devices" fungieren können, können innerhalb des Maschinen-Netzwerkes eingesetzt werden, ohne direkt an das Automatisations-Netzwerk angeschlossen zu sein. Das eigentliche Maschinen-Netzwerk ist maschinen- und geräteindividuell. Es kann daher nur anhand von Beispielen skizziert werden.

1.4 Hinweise zu diesem Dokument

Dieses Handbuch ist Teil des Produktes. Es ist über seine gesamte Lebensdauer aufzubewahren und gegebenenfalls an nachfolgende Besitzer:innen oder Benutzer:innen des Produkts weiterzugeben. Die für Endkunden notwendigen Sicherheitshinweise und Informationen müssen vom Maschinenbauer oder Systemanbieter in die Betriebsanleitung für Endkunden in der jeweiligen Landessprache übernommen werden.

Die Dokumentation muss in einem leserlichen Zustand dem definierten Personenkreis zugänglich gemacht und von diesem gelesen und verstanden werden.

Information

Dieses Handbuch gilt auch für baugleiche und funktional idente Kundenvarianten.

Da sich solche Kundenvarianten mitunter im Aussehen (z.B. durch eine andere Frontfolie) von der KEBA-Standardvariante unterscheiden, können sich die in diesem Handbuch abgebildeten Geräte in ihrem Aussehen von den von Ihnen verwendeten Geräten unterscheiden.

Information

Bei Abweichungen von Kundenvarianten gegenüber der KEBA-Standardvariante kann ein Kundendatenblatt von KEBA bezogen werden.

1.4.1 Inhalt des Dokuments

- Sicherheitshinweise

KEBA © KEBA 2021

- Allgemeine Produktbeschreibung
- Anzeigen, Bedienelemente und Tastatur
- Anschluss und Verdrahtung
- Konfiguration und Bedienhinweise
- Optionen
- Zubehör
- Technische Daten
- CE-Konformität, Richtlinien und Normen

1.4.2 Im Dokument nicht enthalten

- Maskenbeschreibungen der Applikation
- Applikationsspezifische Branchensoftware

1.5 Weiterführende Dokumentation

Dok.Nr.	Bezeichnung	Zielgruppe
1008551	KVC Protokoll	Inbetriebnehmer, Programmierer
1008882	Modbus Protokoll	Inbetriebnehmer, Programmierer
	ADS Protokoll	Inbetriebnehmer, Programmierer
	OPC UA Protokoll	Inbetriebnehmer, Programmierer
	S7 Protokoll	Inbetriebnehmer, Programmierer
	Quick Start Guide	Inbetriebnehmer, Programmierer

Eventuell benötigte Zertifikate (z.B. UL-Zertifikat) können bei KEBA auf Anfrage bezogen werden bzw. sind in der UL Produkt Datenbank gelistet.

1.6 Konformität der sicheren Feldbusse

1.6.1 EtherCAT Erklärungen

EtherCAT®	EtherCAT® ist eine eingetragene Marke und patentierte Technologie, lizenziert durch die Beckhoff Automation GmbH, Deutschland.
Safety over EtherCAT®	Safety over EtherCAT® ist eine eingetragene Marke und patentierte Technologie, lizenziert durch die Beckhoff Automation GmbH, Deutschland.

© KEBA 2021

1.6.2 PROFINet / PROFIsafe Erklärungen

	PROFINet® ist eine eingetragene Marke. Eine Verwendung ist nur für Mitglieder von "PROFIBUS & PROFINET International" erlaubt. Mehr Informationen über die Nutzungsbedingungen sind auf der Web Seite www.profibus.com zu finden.
	PROFIsafe® ist eine eingetragene Marke. Eine Verwendung ist nur für Mitglieder von "PROFIBUS & PROFINET International" erlaubt. Mehr Informationen über die Nutzungsbedingungen sind auf der Web Seite www.profibus.com zu finden.

1.7 Information in Bezug auf MRL 2006/42/EG

Dieses Projektierungshandbuch entspricht der Maschinenrichtlinie 2006/42/EG.

1.7.1 Quantitative Sicherheitsangaben für Not-Halt und Zustimmeinrichtung

Not-Halt und Zustimmtaster

KEBA spezifiziert eine Kategorie und einen PL nach EN ISO 13849-1, sowie einen PFH_D-Wert und eine SIL Einstufung nach EN 61508.

Information

Zustimmtaster- und Nothaltkreise bestehen aus einer Kombination von mechanischen Elementen und elektronischen Auswertungen.

1.7.2 Beziehung zwischen Performance Level und Safety Integrity Level

Tabelle 3 (lt. EN ISO 13849-1:2015) - Beziehung zwischen dem Performance Level (PL) und dem Sicherheits-Integritätslevel (SIL)

Performance Level (PL) nach EN ISO 13849-1	Safety Integrity Level (SIL) nach EN 61508-1
a	keine Entsprechung
b	1
c	1
d	2
e	3

KEBA © KEBA 2021

Tabelle 2 (lt. EN ISO 13849-1:2015) - Performance Level (PL)

Performance Level (PL)	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde 1/h
a	≥ 10^{-5} bis < 10^{-4}
b	≥ 3 x 10^{-6} bis < 10^{-5}
c	≥ 10^{-6} bis < 3 x 10^{-6}
d	≥ 10^{-7} bis < 10^{-6}
e	≥ 10^{-8} bis < 10^{-7}

1.7.3 Abkürzungen

Abkürzung	Englischer Begriff	Deutsche Erklärung
B_{10D}	-	Anzahl von Zyklen, bis 10% der Komponenten gefahrbringend ausfallen (je Kanal)
$MTTF_D$	Mean time to Failure Dangerous	Mittlere Zeit bis zum gefahrbringenden Ausfall (je Kanal)
DC	Diagnostic Coverage	Diagnosedeckungsgrad
PL	Performance Level	Diskreter Level, der die Fähigkeit von sicherheitsgerichteten Geräten angibt, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen.
PFH_D	Probability of Failure per Hour Dangerous	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde
SIL	Safety Integrity Level	Sicherheits-Integritätslevel
t_{Zyklus}	-	Mittlere Zeit zwischen zwei aufeinander folgenden Zyklen in Sekunden
h_{op}	-	Mittlere Betriebszeit in Stunden pro Tag (0 - 24 Stunden)
d_{op}	-	Mittlere Betriebszeit in Tagen pro Jahr (0 - 365 Tage)
n_{op}	-	Mittlere Zahl an Schaltspielen pro Jahr

1.8 Not-Halt-Schalter

Der Not-Halt am Handbediengerät und an der Basisstation entspricht den Anforderungen der EN ISO 13850. Seine Wirkungsweise muss anhand der Risikobeurteilung für die Maschine als Stopp der Kategorie 0 oder der Kategorie 1 ausgebildet werden (siehe EN 60204-1). Die Verschaltung der Relaiskontakte muss jener Kategorie (nach EN ISO 13849-1) genügen, welche anhand der Risikoanalyse (nach EN ISO 12100:2010) der Maschine festgelegt wird.

© KEBA 2021

WARNUNG!

- Nicht funktionstüchtige Not-Halt-Einrichtungen können fatale Folgen haben! Rot-gelb gekennzeichnete Not-Halt-Schalter müssen jederzeit und in allen Betriebsarten einer Maschine oder Anlage wirksam sein.
- Ein Entriegeln der Not-Halt-Einrichtung darf keinen unkontrollierten Wiederanlauf bewirken.
- Der Not-Halt ist kein Ersatz für Sicherheitseinrichtungen.
- Bestimmte mechanische Fehler im Not-Halt können nur bei Betätigung erkannt werden.
  Nach heftiger Stoßeinwirkung auf das Gerät (z.B. durch Schlageinwirkung), muss der Not-Halt-Schalter auf Funktionsfähigkeit überprüft werden.
  Zusätzlich muss der Not-Halt zyklisch (alle 1 Monate) durch Betätigen des Not-Halt-Schalters getestet werden.
- Für weitere Informationen zum Not-Halt ist unbedingt auch Kap. "EU-Richtlinien, Normen und Verordnungen" zu beachten.

KEBA © KEBA 2021

2 Sicherheitshinweise

2.1 Darstellung

Im Handbuch finden Sie an verschiedenen Stellen Hinweise und Warnungen vor möglichen Gefahren. Die verwendeten Symbole haben folgende Bedeutung:

GEFAHR!

bedeutet, dass Tod oder schwere Körperverletzung eintreten werden, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

WARNUNG!

bedeutet, dass Tod oder schwere Körperverletzung eintreten können, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

VORSICHT!

bedeutet, dass leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

Achtung

bedeutet, dass ein Sachschaden eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

ESD

Mit dieser Warnung wird auf die möglichen Folgen beim Berühren von elektrostatisch empfindlichen Bauteilen hingewiesen.

Sicherheitsinformation

Beschreibt wichtige sicherheitsrelevante Anforderungen oder informiert über wesentliche sicherheitstechnische Zusammenhänge.

Information

Kennzeichnet Anwendungstipps und nützliche Informationen. Es sind keine Informationen enthalten, die vor einer gefährlichen oder schädlichen Funktion warnen.

© KEBA 2021

2.2 Allgemeine Sicherheitshinweise

Das Handterminal wurde unter Beachtung der ergonomischen Gestaltungsleitsätze sowie den einschlägigen Sicherheitsnormen entwickelt, gefertigt, geprüft und dokumentiert. Bei Beachtung der für den bestimmungsgemäßen Gebrauch beschriebenen Anweisungen und sicherheitstechnischen Hinweise gehen deshalb vom Produkt im Normalfall keine Gefahren in Bezug auf Sachschäden oder für die Gesundheit von Personen aus.

Die in diesem Handbuch enthaltenen Anweisungen müssen in jedem Fall genau befolgt werden. Andernfalls können Gefahrenquellen geschaffen oder die integrierten Sicherheitseinrichtungen unwirksam gemacht werden.

Unabhängig von den in diesem Handbuch angeführten Sicherheitshinweisen sind die dem jeweiligen Einsatzfall entsprechenden Arbeitssicherheits- und Unfallverhütungsvorschriften zu beachten.

Handhabung der Geräte

Um Fehlfunktionen oder Beschädigungen durch unsachgemäße Handhabung zu vermeiden, beachten Sie unbedingt nachfolgende Hinweise beim Betrieb der Geräte:

WARNUNG!

Folgende Anwendungsbereiche sind für das KeTop ohne besondere Bewertung in Zusammenhang mit der Anwendung und erforderliche Maßnahmen in der Installation bezüglich der Betriebsbedingungen, ausdrücklich ausgeschlossen:

- Einsatz in explosions- bzw. feuergefährdeten Bereichen
- Einsatz im Bergbau
- Einsatz im Freien

Für diese Anwendungen sind spezielle, für die jeweiligen Umgebungen bestimmte Produkte anzuwenden!

ESD

Das Gehäuse darf nicht geöffnet werden, da das Gerät im geöffneten Zustand empfindlich gegen elektrostatische Entladung ist.

Information

Dieses Produkt wurde für den Einsatz im Industriebereich entwickelt und kann bei Einsatz im Wohnbereich Funkstörungen verursachen.

KEBA © KEBA 2021

Achtung

Zerstörung der Geräte oder des Steuerungssystems bei unsachgemäßer Handhabung!

Die Geräte dürfen nur bei abgeschalteter Versorgungsspannung ein- und ausgebaut werden. Andernfalls können die Geräte zerstört werden oder undefinierte Signalzustände können zu Schäden führen.

Damit die Geräte bei einem Weiter- oder Rücktransport keinen Schaden nehmen, muss für den Transport immer die Originalverpackung verwendet werden.

Achtung

- Achten Sie darauf, dass das Handbediengerät nicht auf der Bedienseite abgelegt wird und dadurch Bedienelemente mechanisch beschädigt oder ungewollt betätigt werden.
- Legen Sie das Handbediengerät niemals auf instabile Oberflächen / Ablagen. Es könnte herunterfallen und dadurch Schaden nehmen.
- Montieren/Stellen Sie die Geräte niemals in die Nähe von Wärmequellen oder direkter Sonneneinstrahlung.
- Vermeiden Sie, dass die Geräte mechanischen Erschütterungen, übermäßig viel Staub, Feuchtigkeit oder starken Magnetfeldern ausgesetzt werden.
- Vermeiden Sie die Kabelführung über scharfe Kanten, wodurch der Kabelmantel aufgescheuert werden kann.
- Verhindern Sie, dass Fremdkörper oder Flüssigkeiten in das Geräteinnere gelangen. Kontrollieren Sie periodisch und insbesondere nach schweren Erschütterungen (z.B. Fall) die am Gerät vorhandenen Schutzabdeckungen, die Vollständigkeit der Gehäuseverschraubung sowie Beschädigungen am Gehäuse und Kabeldurchführung.
- Sollte das Gerät einen Fehler haben, nehmen Sie es außer Betrieb und senden Sie es bitte mit einer detaillierten Fehlerbeschreibung an Ihren Lieferanten oder an die vereinbarte Serviceniederlassung.
- Legen/hängen Sie das Gerät, falls vorhanden, in die dafür vorgesehene Ladestation, wenn Sie es nicht benützen.
- Das Handbediengerät darf keinesfalls mit spitzen Gegenständen (z.B. Schraubendreher,...) bedient werden, da dies zur Zerstörung des Geräts führt. Bedienen Sie das Gerät mit dem Finger oder mit einem Touchstift.
- Der Anschlussschacht darf nur beim abgeschalteten Gerät geöffnet werden. Andernfalls können Bauteile zerstört werden oder undefinierte Signalzustände auftreten.

© KEBA 2021

2.3 Sicherheitshinweise zur Personensicherheit

WARNUNG!

Personengefährdung durch elektrischen Schlag!

- Laden Sie das Handbediengerät bzw. versorgen Sie die Basisstation ausschließlich aus Spannungsquellen, welche Schutzkleinspannung aufweisen (z.B. SELV oder PELV nach EN 61010-2-201).
- Durch das Anschließen einer SELV Spannungsquelle kann diese, bedingt durch die Bauart, zu einer PELV Spannungsquelle werden.
- Schließen Sie an Anschlüsse, Klemmen oder Schnittstellen bis 50 V Nennspannung nur Spannungen und Stromkreise an, welche eine sichere Trennung zu gefährlichen Spannungen haben (z.B. durch ausreichende Isolierung und Spannungsfestigkeit).

VORSICHT!

Brandgefahr bei Bauteilausfall!

Sorgen Sie bei der Versorgung der Basisstation für eine angemessene Absicherung der 24 V DC Stromversorgung des Gerätes! Es muss dazu eine UL 248 zugelassene Sicherung mit max. 3,15 A verwendet werden.

Laden Sie das Handbediengerät nur mit den seitens KEBA empfohlenen Ladegeräten und mit den vorgesehenen Lademitteln (Ladestation und Netzteil).

KEBA © KEBA 2021

WARNUNG!

- Die richtige Projektierung des Systems ist durch den Maschinenhersteller aufgrund der Risikobeurteilung durchzuführen. Folgende Sicherheitsaspekte müssen unter anderem hierfür überlegt werden:
  - Richtige Arbeitsbereichseinschränkung (optional mit Bedienbereichsüberwachungsmodul)
  - Not-Halt Konzept notwendig
  - Kategorie und Performance-Level für die jeweilige Anwendung ausreichend
- Von der Bedienstelle, die vom Personal eingenommen wird, muss Einsicht in die Gefahrenstelle gegeben sein.
- Die Basisstation darf nicht im Gefahrenbereich der Maschine montiert werden. (Siehe 5.7.1 Positionierung der Basisstation.)
- Die Geräte dürfen nur in einwandfreiem Zustand und unter Beachtung der Betriebsanleitung betrieben werden.
- Wenn Not-Halt-Geräte auf kabellosen Bedienstationen (z.B. drahtlose Programmiergeräte) angebracht sind, dann muss mindestens ein Not-Halt-Gerät immer an der Maschine verfügbar sein.
- Nicht verwendete (nicht angeschlossene) Handbediengeräte müssen verstaut werden, damit keine Verwechslungsgefahr mit einem angeschlossenen Handbediengerät entstehen kann.
- Während ein Handbediengerät an der Basisstation an-/abgemeldet wird, darf sich keine Person im Gefahrenbereich der Maschine aufhalten.
- Der Bediener muss dem erforderlichen Ausbildungsniveau genügen, sowie die Einzelheiten der bestimmungsgemäßen Verwendung entsprechend der Bedienungsanleitung kennen.
- Die Sicherheitshinweise und Informationen in den Folgekapiteln sind unbedingt mit zu berücksichtigen.

© KEBA 2021

VORSICHT!

Personengefährdung durch Brandgefahr oder Verätzung!

- Der Akku darf nur für den bestimmten Gebrauch verwendet werden.
- Der Akku darf weder zerlegt, geöffnet noch zerkleinert werden.
- Der Akku darf nicht kurzgeschlossen werden.
- Ladekabel oder Ladeschale dürfen keine Beschädigungen aufweisen.
- Im Falle eines Auslaufens eines Akkus darf die Flüssigkeit nicht mit der Haut oder den Augen in Berührung kommen. Bei Berührung die betroffene Stelle mit reichlich Wasser abwaschen und einen Arzt aufsuchen.
- Der Akku darf keinen mechanischen Schocks, Druck, Schlägen oder punktuellen Belastungen ausgesetzt werden.
- Der Akku darf weder Feuer noch Hitze ausgesetzt werden.
- Der Akku darf keinem Schmutz oder Feuchtigkeit ausgesetzt werden.
- Den Akku darf nicht im Restmüll entsorgt, sondern muss unter Beachtung der nationalen und lokalen Vorschriften dem ordnungsgemäßen Recycling zugeführt werden. Der Akku darf nur vollständig entleert entsorgt werden. Andernfalls müssen die Kontakte mit Klebestreifen isoliert werden, um einen Kurzsschluss zu vermeiden.
- Der Akku darf nur durch einen von KEBA bezogenen Akku getauscht werden. Bei Verwendung eines anderen Akkus besteht Brand- oder Explosionsgefahr.

KEBA © KEBA 2021

Achtung

Ausfall der Akkus durch unsachgemäße Verwendung!

Der Akku muss vor der ersten Verwendung geladen werden.

- Die Lagerung in direkter Sonneneinstrahlung ist zu vermeiden.
- Die Batterie ist an einem kühlen, trockenen und gut belüfteten Ort zu lagern.
- Die Batterie ist in einer staubfreien Umgebung ohne korrosive Gase zu lagern.
- Die Batterie darf nicht länger als 24 Stunden im Ladegerät verbleiben.
- Der Akku muss vor der ersten Verwendung vollständig aufgeladen werden.
- Der Akku darf nur in der Originalverpackung gelagert werden. Behältnisse, in denen Kurzschlüsse mit losen metallischen Gegenständen verursacht werden können, sind zu vermeiden.
- Lagern Sie die Batterie ohne Verpackung nicht in Behältnissen in denen Kurzschlüsse mit losen metallischen Gegenständen verursacht werden können.
- Der Akku darf nicht länger als 1 Monat in entladenem Zustand gelagert werden.

2.4 ESD-Hinweise

Elektronische Bauteile sind generell durch elektrostatische Entladungen (**E**lectro **S**tatic **D**ischarge) gefährdet. Elektrostatische Aufladung kann bei jeder bewegenden Tätigkeit entstehen. ESD kann bei jeder Berührung entstehen.

Die meisten Entladungen sind so gering, dass sie nicht wahrgenommen werden. Sie können aber trotzdem ungeschützte elektronische Bauteile gefährden oder zerstören. Daher ist generell jeder Umgang mit offener Elektronik nur unter wirksamem ESD-Schutz zulässig.

Beachten Sie beim Umgang mit **offener** Elektronik folgende ESD-Maßnahmen:

- Offene Elektronik nur berühren, wenn es unbedingt notwendig ist.
- Ableitungsfähiges ESD-Handgelenksband anlegen.
- Ableitfähige Arbeitsunterlage verwenden.
- Leitende Verbindung zwischen Gerät/System, Unterlage, Handgelenksband und Erdanschluss herstellen.
- Arbeitskleidung aus Baumwolle gegenüber Kunstfasermaterialien bevorzugen.

© KEBA 2021

- Arbeitsbereich von hochisolierenden Materialien (z.B. Styropor, Kunststoffe, Nylon, ...) freihalten.
- Auch bei defekten Baugruppen ESD-Schutz anwenden.

Bewahren Sie generell die Geräte immer in der Originalverpackung auf und entnehmen Sie diese erst unmittelbar vor dem Einbau.

Vermeiden Sie, auch bei Baugruppen, die in ein Gehäuse eingebaut sind, den direkten Kontakt mit eventuell zugänglichen elektronischen Bauteilen, wie zum Beispiel im Bereich nicht bestückter Klemmen.

KEBA © KEBA 2021

3 Systemübersicht

Das Safe Wireless System besteht aus einem oder mehreren Wireless Handbediengeräten und einer oder mehreren Basisstationen. Die Datenübertragung zwischen Handbediengerät und Basisstation erfolgt über Funkverbindungen. Die Funkverbindungen zur Basisstation bestehen einerseits aus einem Kanal zur Übertragung von sicherheitsgerichteten Informationen, auch "sichere Verbindung" genannt, (z.B. für den beleuchteten Not-Halt) über Bluetooth und einem Kanal zur Übertragung von nicht sicherheitsgerichteten Informationen, auch "unsichere Verbindung" genannt, über WLAN. Je nach Konfiguration kann das WLAN der Basisstation oder das WLAN des Hallennetzwerks für die unsichere Verbindung verwendet werden. Die sichere Verbindung besteht zu jedem Zeitpunkt immer nur zwischen genau einem Handbediengerät und einer Basisstation.

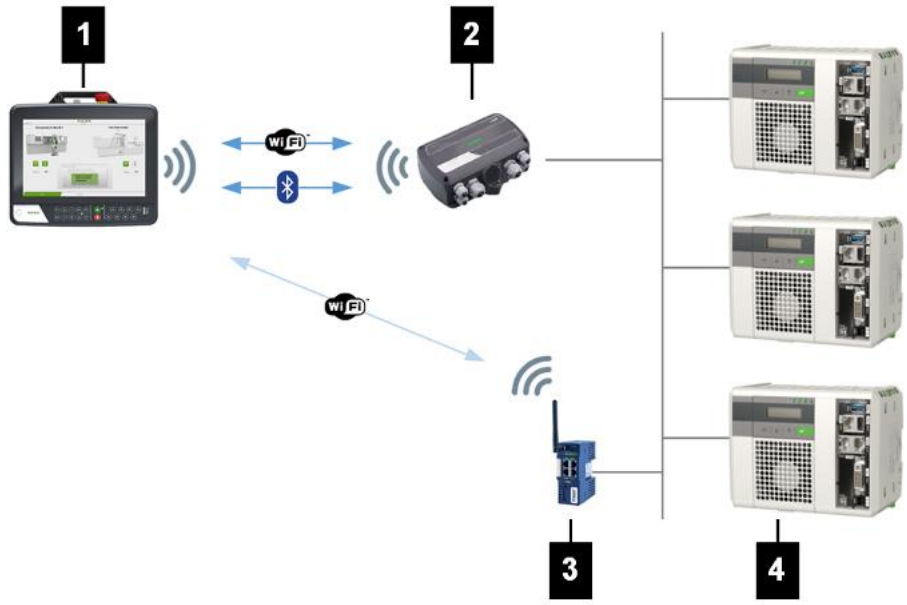


Abb. 3-3: Systemaufbau

1 ... Handbediengerät	2 ... Basisstation
3 ... Hallennetzwerk	4 ... Steuerungen

Betrieb mit "sicherer Verbindung"

Um eine sichere Verbindung aufzubauen, muss ein Handbediengerät mit genau einer Basisstation explizit verbunden ("pairing") werden. Da es sich dabei um eine "Punkt zu Punkt" Verbindung handelt, ist immer genau ein Handbediengerät mit genau einer Basisstation verbunden. Durch die Anordnung der Basisstation(en) muss sichergestellt werden, dass das Handbediengerät nur dort angemeldet werden kann, wo der Benutzer auch Einsicht in die Gefahrenstelle hat.

Es können 10 Systeme (Handbediengerät mit Basisstation) auf einer Fläche von 400 m² parallel betrieben werden.

© KEBA 2021

Die Sicherheitseinrichtungen am Handbediengerät funktionieren nur, wenn eine sichere Verbindung (mittels "Pairing") zur Basisstation aufgebaut wurde.

Je nach Konfiguration können nicht sicherheitsgerichtete Daten über das WLAN der Basisstation oder über das WLAN des Hallennetzwerks übertragen werden.

Nach Beendigung der Arbeiten muss das Handbediengerät von der Basisstation wieder abgemeldet werden. Es kann danach mit einer beliebigen, freien Basisstation erneut verbunden werden.

WARNUNG!

Sind mehr als eine Basisstation an einer Maschine vorhanden, so muss sichergestellt werden, dass nur eine Kombination (Basisstation/Handbediengerät) auf die Maschine wirkt. Gegebenenfalls müssen die Basisstationen gegeneinander verriegelt werden ("Single Point of Control"). Dies muss im übergeordneten Sicherheitskonzept realisiert werden.

Betrieb mit "unsicherer Verbindung" (funktionale Verbindung)

Im Betrieb mit "unsichere Verbindung" wird das Handbediengerät nur mit dem WLAN des Hallennetzwerks verbunden. Die Sicherheitseinrichtungen am Handbediengerät stehen nicht zur Verfügung. Es ist nur ein Datenaustausch von funktionalen Daten möglich. Dieser erfolgt über die konfigurierte WLAN-Verbindung im Hallennetzwerk. Eine Übertragung von sicheren Daten ist nicht möglich. Ein An- bzw. Abmelden an einer Basisstation ist für diesen Betriebsfall nicht notwendig.

3.1 Bedienbereichsüberwachung / BBÜ (optional)

Information

Die Bedienbereichsüberwachung kann auf Wunsch auch nachträglich von KEBA implementiert werden.

Damit keine gefährlichen Aktionen der Maschine bzw. von Maschinenteilen außerhalb des Sichtbereiches der Gefahrenstelle ausgelöst werden können, ist eine Bedienbereichsüberwachung verfügbar. Die Bedienbereichsüberwachung bietet zusätzlich den Vorteil, die Wahrscheinlichkeit von Verbindungsabbrüchen zu reduzieren. Solange sich der Bediener im eingestellten Bedienbereich befindet, ist die Bedienbereichsüberwachung für den Benutzer nicht wahrnehmbar. Durch taktile und optische Maßnahmen (Vibration des Handbediengerätes und Pulsieren des beleuchteten Nothalts), wird der Bediener darauf hingewiesen, dass er die Grenze des Bedienbereichs überschritten hat und sich im Toleranzbereich befindet. Bewegt sich der Bediener dann weiter in den Übertretungsbereich, erhöht sich die Frequenz dieser

KEBA © KEBA 2021

Maßnahmen. Im umgekehrten Fall reduziert sich die Frequenz. Die Verfügbarkeit der Sicherheitsfunktionen in diesen drei Zonen, ist in diesem Kapitel beschrieben.

Information

Ist die Bedienbereichsüberwachung aktiv, sind zusätzliche Hinweise zum Pairing/Unpairing zu beachten (siehe 11 Verbinden mit Basisstation).

WARNUNG!

Verletzungsgefahr durch nicht einsehbare Gefahrenstellen

Die Bedienbereichsüberwachung misst den Abstand zwischen Handbediengerät und Basisstation. Der Bedienbereich der Anlage muss so gestaltet sein, dass innerhalb dieses Abstandes Einsicht in die Gefahrenstelle besteht. Auch im Toleranzbereich muss Einsicht in Gefahrenstellen gegeben sein!

Die Abstandsmessung der Bedienbereichsüberwachung ist bei der Inbetriebnahme bzw. beim Ändern des Arbeitsbereiches zu validieren und muss zyklisch (alle 1 Monate) auf ihre Funktion überprüft werden (siehe 10.1 Validierung der Abstandsmessung).

Die Abstrahlcharakteristik der Bedienbereichsüberwachung ist halbkugelförmig vor der Basisstation. Somit ist die richtige Positionierung der Basisstation für die Effizienz und Genauigkeit des Systems sehr wichtig (siehe 5.7.1 Positionierung der Basisstation).

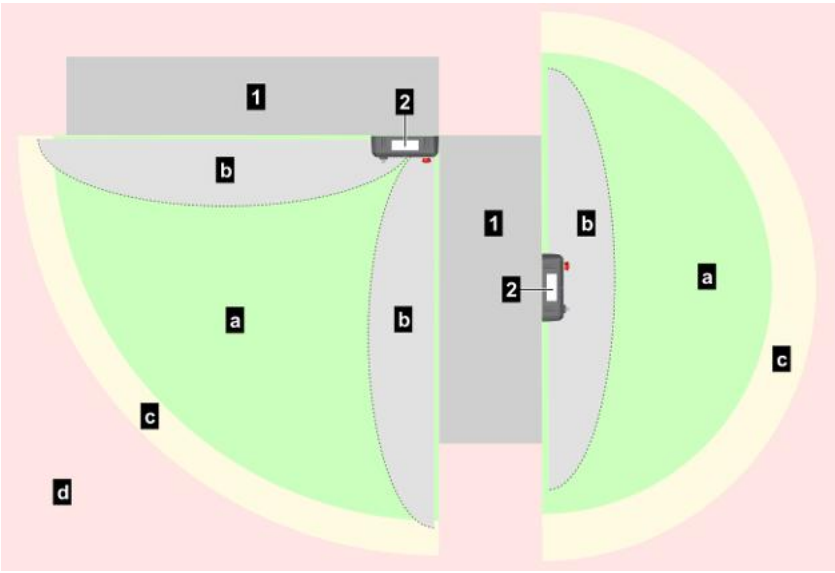


Abb. 3-4: Installationsbeispiel Grundriss

1 ... Maschine	2 ... Basisstation
a ... Eingestellter Bedienbereich	b ... Vorgesehener Arbeitsbereich
c ... Toleranzbereich	d ... Übertretungsbereich

© KEBA 2021

Der maximal parametrierbare Bedienbereich beträgt 20 m und kann auf der Basisstation über DIP-Switches konfiguriert werden (siehe 8.3 Bedienbereichs-Konfiguration (sicherheitsrelevant)).

Der Kommunikationskanal der Bedienbereichsüberwachung wird in der Gerätekonfiguration automatisch festgelegt und kann gegebenenfalls am Handbediengerät eingestellt (siehe 8.4.5 Network) werden. Nach erfolgreicher Einstellung wird die zusätzliche Funkverbindung automatisch aufgebaut und startet die Überwachung.

Auf einer Fläche von 500 m^2 können parallel bis zu 5 Verbindungen (Handbediengerät und Basisstation) mit Bedienbereichsüberwachung betrieben werden.

Zonen der Bedienbereichsüberwachung

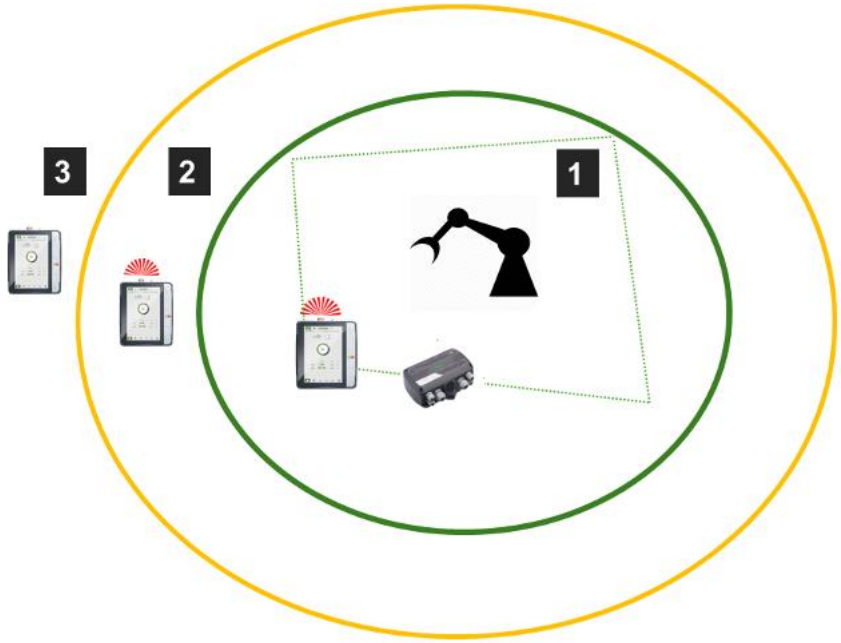


Abb. 3-5: Zonen der Bedienbereichsüberwachung

1 ... Bedienbereich	2 ... Toleranzbereich
3 ... Übertretungsbereich	

Die grüne durchgezogene Linie stellt die Grenze des Arbeitsbereichs dar, der als Bedienbereich eingestellt wird. Der weitest entfernte Punkt im Arbeitsbereich definiert den Bedienbereich (vergleichbar zur Kabellänge bei kabelgebundenen Geräten).

Die gelbe Linie stellt den Toleranzbereich dar. Der Toleranzwert beträgt standardmäßig 3 m und ist nicht konfigurierbar. Dieser Wert wird zusätzlich zum Radius berücksichtigt.

Um vom Toleranzbereich wieder in den Bedienbereich zu wechseln, muss um 2 m in den definierten Arbeitsbereich eingetreten werden.

KEBA © KEBA 2021

Information

Die Distanzmessung der Bedienbereichsüberwachung ist am genauesten, wenn die Rückseite des Handbediengeräts zur Frontseite der Basisstation gerichtet ist. Wenn das Handbediengerät abgeschirmt wird (z. B. Körper des Bedieners) können aufgrund dessen falsch hohe Distanzwerte vom Messsystem ausgegeben werden, welche zu einem ungewollten Stillstand der Maschine führen können.

Befindet sich das Handbediengerät nicht in einem halbkugelförmigen Bereich vor der Basisstation, können falsch hohe Distanzwerte vom Messsystem ausgegeben werden, welche zu einem ungewollten Stillstand der Maschine führen können.

Wird das Handbediengerät wie hier beschrieben ausgerichtet und ein Mindestabstand von 3 m eingehalten, erreicht dieses System eine Messtoleranz von +/- 1 m. Auch bei nicht optimaler Ausrichtung wird die Messtoleranz von - 1 m nicht unterschritten.

Bedienbereich

Im Bedienbereich ist im verbundenen Zustand ein vollständiger Funktionsumfang gegeben. Der Not-Halt ist beleuchtet und funktionsfähig. Der Zustimmtaster ist ebenfalls funktionsfähig.

Toleranzbereich

Ein Betreten des Toleranzbereichs wird durch Vibration des Handbediengeräts und optische Signale angezeigt. Der Not-Halt ist im Toleranzbereich nicht mehr gleichmäßig beleuchtet, sondern das Licht pulsiert. Er ist aber weiterhin funktionsfähig.

Bei betätigtem Zustimmtaster wird nach ca. 10 sec (nicht einstellbar) der Ausgang weggenommen. Ist beim Betreten des Toleranzbereiches der Zustimmtaster nicht betätigt, kann keine Zustimmung mehr gegeben werden. Nur im Bedienbereich kann durch Loslassen und erneutem Betätigen des Zustimmtasters die Zustimmung gegeben werden.

Übertretungsbereich

Ein Betreten des Übertretungsbereichs (also Verlassen des Toleranzbereichs) wird sofort durch starke Vibration und optische Signale angezeigt.

Die Not-Halt Funktion wird nach ca. 3 sec (nicht einstellbar) ausgelöst und die Beleuchtung des Not-Halts am Handbediengerät wird deaktiviert. Die Maschine geht in sicheren Zustand.

Ein betätigter Zustimmtaster wird unmittelbar bei Betreten des Übertretungsbereichs deaktiviert. Ein nicht betätigter Zustimmtaster kann nicht mehr aktiviert werden.

© KEBA 2021

Kompatibilität

KeTop T15xWL	KeTop CB4xx	Verbindungsaufbau
Mit Bedienbereichsüberwachung	Mit Bedienbereichsüberwachung	Möglich
Ohne Bedienbereichsüberwachung	Ohne Bedienbereichsüberwachung	Möglich
Mit Bedienbereichsüberwachung	Ohne Bedienbereichsüberwachung	Möglich
Ohne Bedienbereichsüberwachung	Mit Bedienbereichsüberwachung	Nicht möglich

3.2 Bestellübersicht

Handbediengerät

	KeTop	T	150	WL	-	R	1	0	-	E	N	0	-	W10E
Produktgruppe	KeTop													
Variantenausprägung														
• KEBA Standard		T												
• Kundenspezifisch (Customized)		C												
Format														
• Hochformat			150											
• Querformat			155											
Wireless				WL										
Folientastatur														
• KEBA Standard-Tastatur						D								
• KEBA Robotik-Tastatur						R								
• Kundenspezifische Bedruckung der KEBA Standard-Tastatur						1								
• Kundenspezifische Tastatur						2								
Passive Bedienelemente neben dem E-Stop montiert (nicht sicherheitsrelevant)							1							
Passive Bedienelemente auf der Frontseite montiert (nicht sicherheitsrelevant)								0						
Funktionale Sicherheit										E				
CPU / SSD-Speicher														
• N2807 + 64 GB											N			
• N2807 + 256 GB											f			
• X6211 + 64 GB											S			

KEBA © KEBA 2021

	KeTop	T	150	WL	-	R	1	0	-	E	N	0	-	W10E
• X6211 + 256 GB											T			
Optionen														
• Ohne Bedienbereichs-überwachung (BBÜ)												0		
• Mit BBÜ 1.0												1		
• Mit BBÜ 2.0												2		
Softwareausprägung														W10E

Basisstation

KeTop CB410-EE1-xxx

	KeTop	CB4	1	0	-	E	E	1	-	xxx
Produktgruppe	KeTop									
Variante		CB4								
Ausgänge Nothalt/Zustimm-taster										
• Relais / Halbleiteraus-gänge			1							
• PROFIsafe			2							
• FSoE			3							
Montageart Basisstation										
• Ohne Kabelauslass				0						
• Mit Kabelauslass				1						
Funktionale Sicherheit										
• inkl. Nothalt Taster						E				
Passives Bedienelement ne-ben dem E-Stop montiert (nicht sicherheitsrelevant)							E			
Konfiguration										
• Pairing/Remotepairing Ausgänge (PO/SPO)								0		
• PO/SPO + funktionale Fast Response outputs (FRB)								1		
• PO/SPO + FRB + Be-dienbereichsüberwa-chung (BBÜ 1.0)								2		
• PO/SPO + Bedienbe-reichsüberwachung (BBÜ 1.0)								3		
• PO/SPO + FRB + Be-dienbereichsüberwa-chung (BBÜ 2.0)								4		

© KEBA 2021

	KeTop	CB4	1	0	-	E	E	1	-	xxx
• PO/SPO + Bedienbereichsüberwachung (BBÜ 2.0)								5		
Kundenspezifisch										
• KEBA										0
• Kunde										xxx

KEBA © KEBA 2021

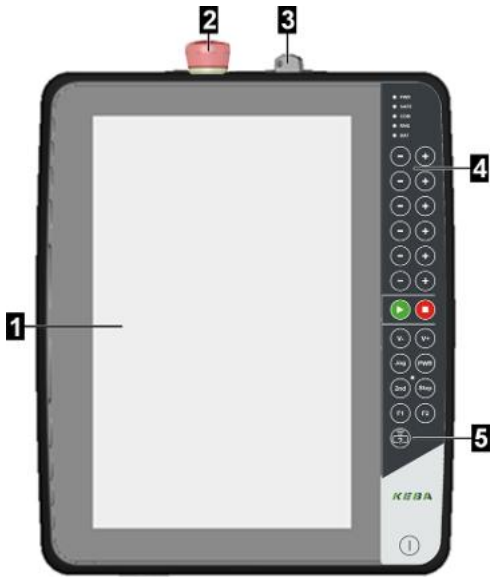
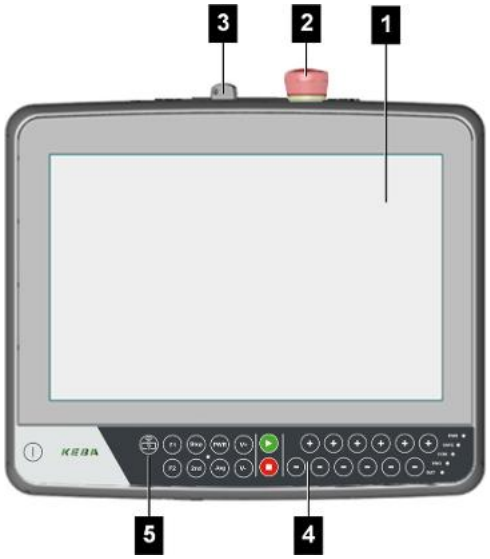
4 Beschreibung der Handbediengeräte

Die Handbediengeräte sind tragbare Bedien- und Anzeigegeräte in robustem Design. Mit dem Farbdisplay können sämtliche Aufgaben grafisch gelöst werden. Der Touchscreen ermöglicht eine intuitive Bedienung. Über die mitgelieferte Ladestation können die Handbediengeräte geladen und verwahrt werden.

Durch optionale Bedien- und Steuerelemente können die Geräte einfach an den jeweiligen Einsatzfall angepasst werden.

Die Auswahl des für die Maschine geeigneten Handbediengeräts sowie die Projektierung der möglichen Zusatzoptionen muss ausgehend von der gesetzlich erforderlichen Gefahren- und Risikobeurteilung im Verantwortungsbereich des Maschinenherstellers erfolgen.

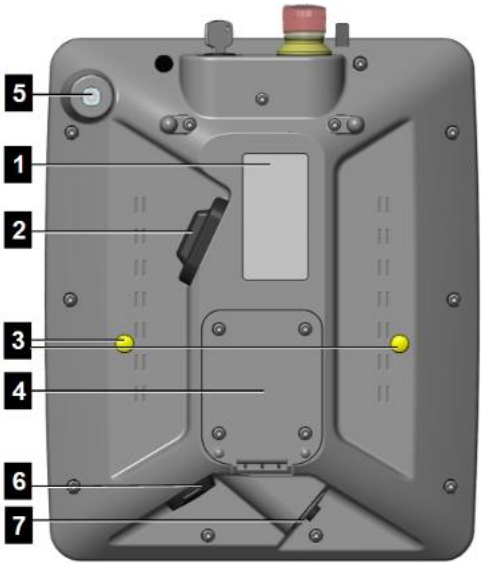
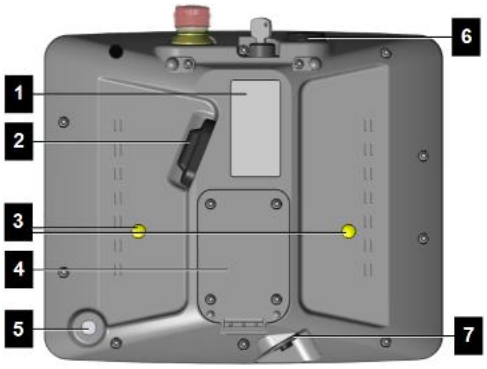
4.1 Frontansicht

T150WL	T155WL
	

1 ...	TFT-Display mit projiziert-kapazitivem Multitouchscreen	2 ...	Beleuchteter Not-Halt
3 ...	Einbauplatz für Optionen	4 ...	Folientastatur
5 ...	"Ident"-Taster		

© KEBA 2021

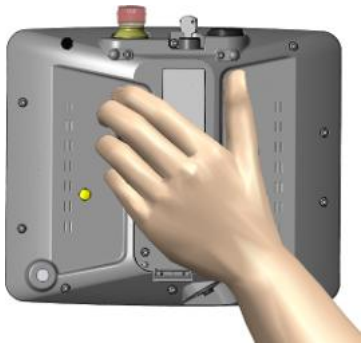
4.2 Rückansicht

T150WL	T155WL
	

1 ...	Typenschild	2 ...	Zustimmtaster
3 ...	Ladekontakte	4 ...	Anschlussschachtdeckel
5 ...	Kamera (optional)	6 ...	USB-Port
7 ...	Externe Spannungsversorgung (DC-Buchse passend für DC-Hohlstecker 5.5/2.1)		

4.3 Handhabung

Das Handbediengerät wird mit der linken Hand gehalten. Dabei kann mit den Fingern der Zustimmtaster betätigt werden. Mit der anderen Hand können dann der Touchscreen und die Tastatur bedient werden.

T150WL	T155WL
	

KEBA © KEBA 2021

4.4 Typenschild

Das Typenschild befindet sich auf der Rückseite des Handbediengeräts. Es enthält produktspezifische Angaben sowie technische und regulatorische Kennzeichnungen.

Die folgenden Abschnitte zeigen die Typenschilder der jeweiligen Gerätevarianten.

4.4.1 Typenschild Celeron N2807

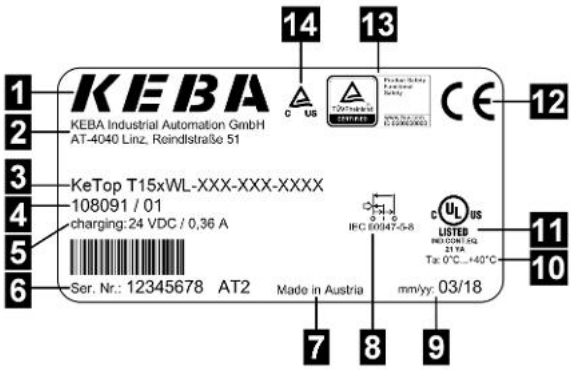


Abb. 4-6: Typenschild

1 ... Hersteller	2 ... Herstelleradresse
3 ... Produktbezeichnung	4 ... Material- / Revisionsnummer
5 ... Technische Daten (Spannung / Strom)	6 ... Seriennummer
7 ... Herstellungsland	8 ... Norm und Symbol 3-stufige Zustimmeinrichtung
9 ... Produktionsdatum	10 ... Umgebungstemperatur
11 ... UL-Prüfzeichen	12 ... CE-Konformitätskennzeichnung
13 ... TÜV-Prüfzeichen	14 ... cTÜVus-Prüfzeichen

© KEBA 2021

4.4.2 Typenschild Intel Atom x6211

KeTop mit Bedienbereichsüberwachung (BBÜ)

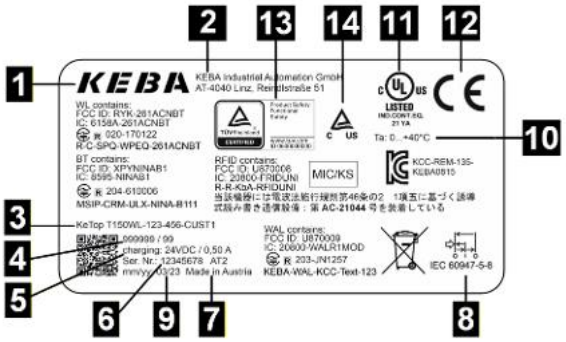


Abb. 4-7: Typenschild KeTop mit BBÜ

1 ... Hersteller	2 ... Herstelleradresse
3 ... Produktbezeichnung	4 ... Material- / Revisionsnummer
5 ... Technische Daten (Spannung / Strom)	6 ... Seriennummer
7 ... Herstellungsland	8 ... Norm und Symbol 3-stufige Zustimmeinrichtung
9 ... Produktionsdatum	10 ... Umgebungstemperatur
11 ... UL-Prüfzeichen	12 ... CE-Konformitätskennzeichnung
13 ... TÜV-Prüfzeichen	14 ... cTÜVus-Prüfzeichen

KeTop ohne Bedienbereichsüberwachung (BBÜ)

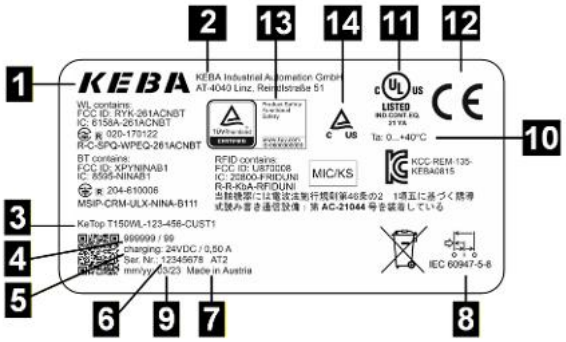


Abb. 4-8: Typenschild KeTop ohne BBÜ

1 ... Hersteller	2 ... Herstelleradresse
3 ... Produktbezeichnung	4 ... Material- / Revisionsnummer
5 ... Technische Daten (Spannung / Strom)	6 ... Seriennummer
7 ... Herstellungsland	8 ... Norm und Symbol 3-stufige Zustimmeinrichtung
9 ... Produktionsdatum	10 ... Umgebungstemperatur

© KEBA 2021

11 ... UL-Prüfzeichen	12 ... CE-Konformitätskennzeichnung
13 ... TÜV-Prüfzeichen	14 ... cTÜVus-Prüfzeichen

4.5 Anzeigen und Bedienelemente

- Folientasten mit mechanischem Druckpunkt
- Status LEDs
- Kapazitiver Multi-Touch-Screen mit Finger bedienbar
- Hintergrundbeleuchtetes Farb-LED-Display

Achtung

Tastaturbeschädigung bei unsachgemäßer Behandlung!

- Keine Bedienung der Tastatur mit spitzen, scharfen, metallischen Gegenständen und auch nicht mit Kugelschreibern oder Bleistiften.
- Zu festes Drücken der Tasten kann diese beschädigen.

4.5.1 Standardtastatur

KeTop T150WL

Variante der Folientastatur, bestückt mit 22 Tasten und 5 Status-LEDs.

Abb. 4-9: Standardtastatur, frontseitig

© KEBA 2021

KeTop T155WL

Variante der Folientastatur, bestückt mit 22 Tasten und 5 Status-LEDs.

Abb. 4-10: Standardtastatur, frontseitig

Variante der Folientastatur mit Ausnehmung für optionales Einbauelement (z.B. Handrad), bestückt mit 22 Tasten und 5 Status-LEDs.

Abb. 4-11: Standardtastatur mit Ausnehmung, frontseitig

4.5.2 Robotik-Tastatur

KeTop T150WL

Folientastatur, bestückt mit 24 Tasten und 5 Status-LEDs.

Information

Das Handbediengerät T150WL ist standardmäßig mit der Robotik-Tastatur ausgerüstet.

© KEBA 2021

Abb. 4-12: Robotik-Tastatur, frontseitig

Variante der Folientastatur mit Ausnehmung für optionales Einbauelement (z.B. Handrad), bestückt mit 24 Tasten und 5 Status-LEDs.

© KEBA 2021

Abb. 4-13: Robotik-Tastatur mit Ausnehmung, frontseitig

KeTop T155WL

Folientastatur, bestückt mit 24 Tasten und 5 Status-LEDs.

Abb. 4-14: Robotik-Tastatur, frontseitig

Variante der Folientastatur mit Ausnehmung für optionales Einbauelement (z.B. Handrad), bestückt mit 24 Tasten und 5 Status-LEDs.

Abb. 4-15: Robotik-Tastatur mit Ausnehmung, frontseitig

4.5.3 CNC-Tastatur

Variante der Folientastatur, bestückt mit 20 Tasten und 5 Status-LEDs.

© KEBA 2021

Abb. 4-16: CNC-Tastatur, frontseitig

4.5.4 Status-LEDs

Das mobile Handbediengerät ist mit folgenden LEDs bestückt:

PWR (Spannungsversorgung)

LED	Beschreibung
Dunkel	Keine Versorgungsspannung (z.B. Akku leer)
Grün blinkend	Versorgungsspannung vorhanden, Gerät abgeschaltet
Grün	Versorgungsspannung vorhanden, Gerät betriebsbereit

SAFE (Sichere Verbindung)

LED	Beschreibung
Dunkel	Gerät ist nicht mit einer Basisstation verbunden
Grün	Gerät ist mit einer Basisstation dauerhaft verbunden ("gepairt")

Information

Eine leuchtende SAFE LED signalisiert, dass das Handbediengerät mit einer Basisstation sicher verbunden ("gepairt") ist, auch wenn keine aktive Funkverbindung besteht.

RNG (Bedienbereichsüberwachung)

LED	Beschreibung
Dunkel	Keine Bedienbereichsüberwachung konfiguriert oder verfügbar
Grün	Bedienbereichsüberwachung aktiv

COM (WLAN)

LED	Beschreibung
Dunkel	Keine WLAN-Verbindung aufgebaut
Grün	Bestehende WLAN-Verbindung

BAT (Akku)

LED	Beschreibung
Dunkel	Akku vollständig geladen oder Gerät in Betrieb

© KEBA 2021

LED	Beschreibung
Grün	Akku des Geräts wird geladen
Grün blinkend	Akku kann nicht geladen werden. Kein Akku vorhanden / Akku beschädigt / Unterspannung / Temperatur >45°C

4.5.5 "Ident"-Taster

Der "Ident"-Taster dient zum Identifizieren, mit welcher Basisstation das betriebsbereite Handbediengerät verbunden ist.

Durch längeres Drücken (> 3 sec) des "Ident"-Tasters wird ein Dialog geöffnet, der anzeigt, ob bzw. mit welcher Basisstation das Handbediengerät verbunden ist. Wird der Button nur kurz gedrückt, wird auf der verbundenen Basisstation ein Blinkmuster am LED-Balken angezeigt.

4.5.6 Touchscreen

Zum Einsatz kommt ein projiziert-kapazitiver Multi-Touchscreen.

Achtung

Sachschaden durch Überbeanspruchung des Bildschirms!

Ein Einbrenneffekt kann bei LC-Displays auftreten, wenn ein statisches Bild oder eine ständig wiederholte Grafik über einen längeren Zeitraum angezeigt wird.

Der Einbrenneffekt kann und soll durch regelmäßiges Wechseln des angezeigten Bildes, durch Verwenden eines Bildschirmschoners sowie Reduzierung von Helligkeit und Kontrast des Displays vorgebeugt werden.

Bedienung

Der Touchscreen kann mit einem oder mehreren Fingern (mit oder ohne Handschuh) bedient werden. Für eine lange Haltbarkeit des Touchscreens ist folgendes zu beachten:

KEBA © KEBA 2021

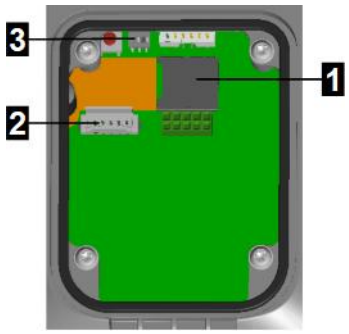
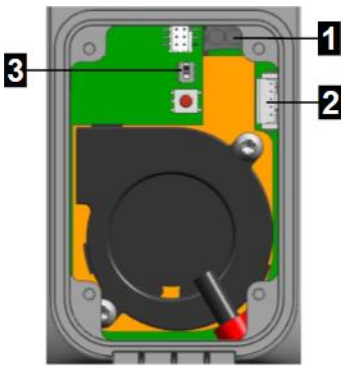
Achtung

Touchbeschädigung bei unsachgemäßer Handhabung!

- Den Touchscreen nur mit einem weichen Tuch mit mildem Reinigungsmittel (z.B. Seifenlauge) reinigen, siehe 13.1 Reinigung des Touchscreens.
- Achten Sie bei der Bedienung mit Handschuhen darauf, dass keine Metallspäne oder scharfe Gegenstände (Späne, Sand, Schleifpaste, etc.) in der bedienenden Fläche des Handschuhs eingebettet sind.
- Keine Bedienung des Touchscreens mit spitzen, scharfen, metallischen Gegenständen und auch nicht mit Kugelschreibern oder Bleistiften.
- Der Touchscreen darf nicht ständigem Sonnenlicht ausgesetzt sein.

4.6 Anschlüsse und Verdrahtung

4.6.1 Anschlussschacht

T150WL	T155WL
	

1 ...	Einschubschacht Micro SD-Karte	2 ...	Stiftleiste - Akkustecker
3 ...	DIP-Switch (8.7 Ruhezustand konfigurieren)		

4.6.2 Akku anstecken

Im Auslieferzustand ist der Akku nicht angesteckt und nur zu 30% geladen. Vor dem Gebrauch muss der Akku vollständig aufgeladen werden.

Nach dem Öffnen des Anschlussschachtes kann der Akku angesteckt werden. Bitte beachten Sie vor dem Öffnen des KeTops folgende Hinweise:

© KEBA 2021

Information

Informationen für das Öffnen des Anschlussschachts:

- Das Handbediengerät mit dem Display nach unten auf einen planen, sauberen und weichen Untergrund auflegen, sodass das Handbediengerät oder dessen Bedienelemente nicht beschädigt werden (z.B. ESD-Matte).
- Verwenden Sie für das Öffnen und Schließen des Anschlussschachts einen Schraubendreher der Type "Torx Größe 10".

Information

Informationen zu Änderungen im Anschlussschacht:

- Beim An- und Abstecken des Akku-Steckers ist darauf zu achten, dass der Stecker durch Ziehen mit den Fingern an seinen Adern abgesteckt wird (keine spitzen Gegenstände dafür zu Hilfe nehmen).

Information

Informationen zum Schließen des Anschlussschachts:

- Die Dichtung muss sauber und unbeschädigt sein und sich an der richtigen Position befinden.
- Es dürfen keine Kabel eingeklemmt werden.
- Der Anschlussschachtdeckel muss mit allen 4 Schrauben wieder verschraubt werden (Drehmoment: 0,8 bis 1,0 Nm). Nur dadurch kann die entsprechende Schutzart wieder gewährleistet werden.

4.6.3 Spannungsversorgung

WARNUNG!

Beachten Sie die sicherheitsrelevanten Hinweise im Kapitel 2.3 Sicherheitshinweise zur Personensicherheit.

Das Handbediengerät wird durch einen Akku mit Spannung versorgt. Der Akku kann entweder über die Ladestation oder über eine externe Spannungsversorgung geladen werden.

4.6.4 Beleuchteter Not-Halt

Der beleuchtete Not-Halt hat die gleiche Funktionalität wie ein rot-gelber Not-Halt. Er ist 2-kreisig verdrahtet und die Kontakte sind als Öffner ausgeführt. Unterschied ist, dass dieser aufgrund der Beleuchtung nur im verbunden (d.h. betriebsbereiten) Zustand als Not-Halt Element erkennbar ist.

KEBA © KEBA 2021

Not-Halt beleuchtet	Not-Halt nicht beleuchtet

Der beleuchtete Not-Halt funktioniert nur, wenn das Handbediengerät mit einer Basisstation verbunden und falls optional ein Bedienbereich konfiguriert ist, sich das Gerät innerhalb des Bedienbereichs befindet.

Der Not-Halt am Handbediengerät entspricht den Anforderungen der EN ISO 13850. Seine Wirkungsweise muss anhand der Risikobeurteilung für die Maschine als Stopp der Kategorie 0 oder der Kategorie 1 ausgebildet werden (siehe EN 60204-1). Die Verschaltung der zwangsöffnenden Relaiskontakte an der Basisstation muss jener Kategorie (nach EN ISO 13849-1) genügen, welche anhand der Risikoanalyse (nach EN ISO 12100:2010) der Maschine festgelegt wird.

WARNUNG!

- Ein Entriegeln der Not-Halt-Einrichtung darf keinen unkontrollierten Wiederanlauf bewirken.
- Der Not-Halt ist kein Ersatz für Sicherheitseinrichtungen.

WARNUNG!

- Der beleuchtete Not-Halt am Handbediengerät ist kein Ersatz für die direkt an der Maschine anzubringenden Not-Halt.
- Bei Verwendung eines beleuchteten Not-Halts ist die Funktionalität und ausreichende Helligkeit bei jedem Verbinden/Abmelden und zyklisch (1 x pro Monat) optisch zu prüfen. Bei unzureichender Helligkeit oder Ausfall der Beleuchtung ist das Handbediengerät zu tauschen.
- In der Endanwendung muss direkte Sonneneinstrahlung auf den beleuchteten Not-Halt vermieden werden, damit der Zustand der Beleuchtung jederzeit erkennbar ist. Bei der Erarbeitung des Maschinen-/Anlagensicherheitskonzeptes ist auch die Lebensdauer der Beleuchtung zu beachten. Im Zuge der Festlegung der Helligkeit der Not-Halt Beleuchtung wurden 1500 LUX nach Arbeitsstättenverordnung zugrunde gelegt.

© KEBA 2021

WARNUNG!

Ist das Handbediengerät starker Verschmutzung ausgesetzt oder kommt es mit kleinen Fremdkörpern in Berührung ist zu beachten, dass die Vertiefung des Not- Halts jederzeit frei ist, damit es zu keiner Beeinträchtigung der Funktion des Schaltelementes kommt.

Bestimmte mechanische Fehler im Not-Halt können nur bei Betätigung erkannt werden. Nach heftiger Stoßeinwirkung auf das Gerät (z.B. durch Fallenlassen) muss der Not-Halt auf Funktionsfähigkeit überprüft werden. Zusätzlich muss der Not-Halt zyklisch (1 x pro Monat) durch Betätigung getestet werden. Bei dieser Prüfung ist auch eine Sichtkontrolle hinsichtlich ev. mechanischer Beschädigungen und starker Verschmutzung bzw. möglicher Funktionsbeeinträchtigung durch Fremdkörper durchzuführen.

Information

Eine defekte Beleuchtung des Not-Halts wird mittels LED-Statusbalken an der Basisstation angezeigt und führt sofort in einen sicheren Zustand.

4.6.5 Zustimmtaster

Das KeTop verfügt über einen Zustimmtaster. Der Zustimmtaster besteht aus einem dreistufigen Bedienelement. Ein wesentliches Merkmal ist die zweikreisige Ausführung und die Zwangsöffnung nach EN 60947-1 und EN 60947-5-8 auf die dritte Schalterstellung.

4.6.5.1 Anforderungen an Zustimmausgänge und Zustimmelektronik

WARNUNG!

Ausgangsseitige Kurzschlüsse können von der Zustimmelektronik nicht erkannt werden. Mittels eines geeigneten Überwachungsgerätes (siehe Kapitel "Anschlussbeispiel mit Überwachungsgerät") kann ein Kurzschluss erkannt werden.

Information

Intern testet die Zustimmelektronik zyklisch auf Kurz- und Querschluss. Bei diesem Selbsttest wird das Zustimmsignal für die Dauer des Testimpulses (max. 1 ms) weggenommen.
Störungen in der Zustimmelektronik werden erkannt und führen zu einem Wegnehmen des Zustimmsignals am Ausgang.

KEBA © KEBA 2021

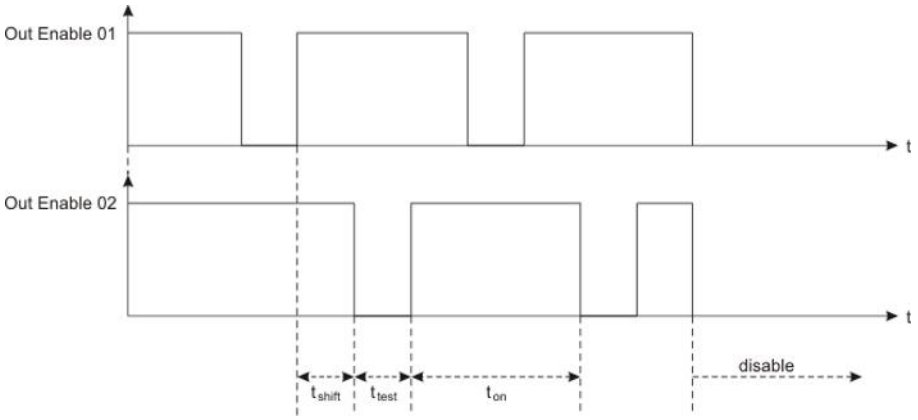


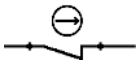
Abb. 4-17: Zustimmelektronik - Prüfung auf Kurz- und Querschluss

Timing und Anforderung

- t_{test}: ≤ 1 ms
- t_{on}: > 400 ms, ≤ 1000 ms

4.6.5.2 Funktionsweise

Der Zustimmtaster kann drei verschiedene Schalterstellungen einnehmen:

Schalterstellung	Funktion	Zustimmtaster	Schaltkontakt
1	Nullstellung	wird nicht betätigt	Aus (geöffnet)
2	Zustimmung	wird betätigt	Ein (geschlossen)
3	Panik	wird durchgedrückt	Aus (geöffnet) 

Entsprechend der EN 60204-1 ist der Zustimmtaster so zu implementieren, dass bei Stellung 1 (Aus-Funktion des Schalters - das Bedienelement ist nicht betätigt) und Stellung 3 (Aus-Funktion - das Bedienelement ist bis zur "Panikstellung" durchgedrückt) mindestens eine der Stopp-Kategorien 0, 1 oder 2 eingeleitet wird.

Für die Berechnung des PL der Sicherheitsfunktion Zustimmung sind die sicherheitstechnischen Kennwerte (PL- und PFH_D-Werte) der involvierten Komponenten mit einzurechnen. Details zur Berechnung des PL für die gesamte Sicherheitsfunktion sind der EN ISO 13849-1 im Kapitel 6.3 sowie dem Anhang H und dem Anhang I zu entnehmen.

WARNUNG!

Der Zustimmtaster muss zyklisch (jeden Monat) durch Betätigen der Panikstellung getestet werden. Es muss überprüft werden, ob die Funktion der Panikstellung gegeben ist.

© KEBA 2021

Normale Betätigung

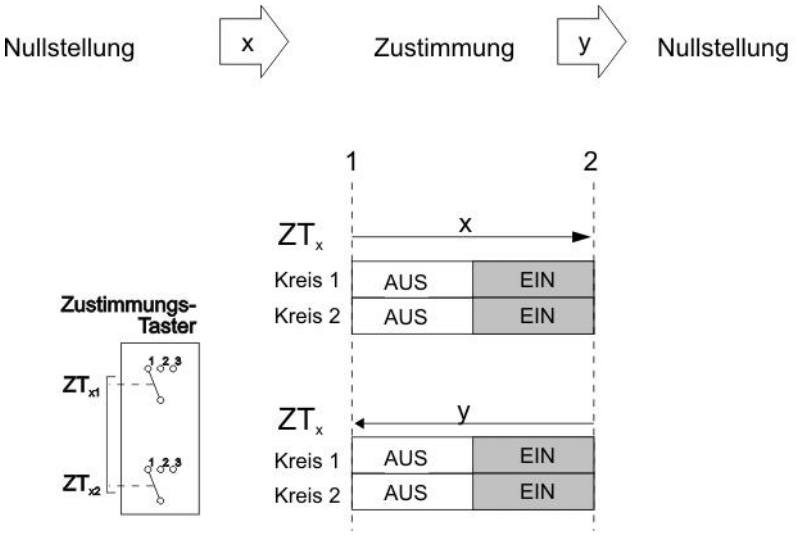


Abb. 4-18: Schaltwegediagramm für normale Betätigung

Panik-Betätigung

Das Schaltelement beim Durchdrücken der Betätigungselemente auf Panik-Stellung ist mechanisch so konstruiert, dass beim Loslassen die Zustimm-Stellung übersprungen wird:

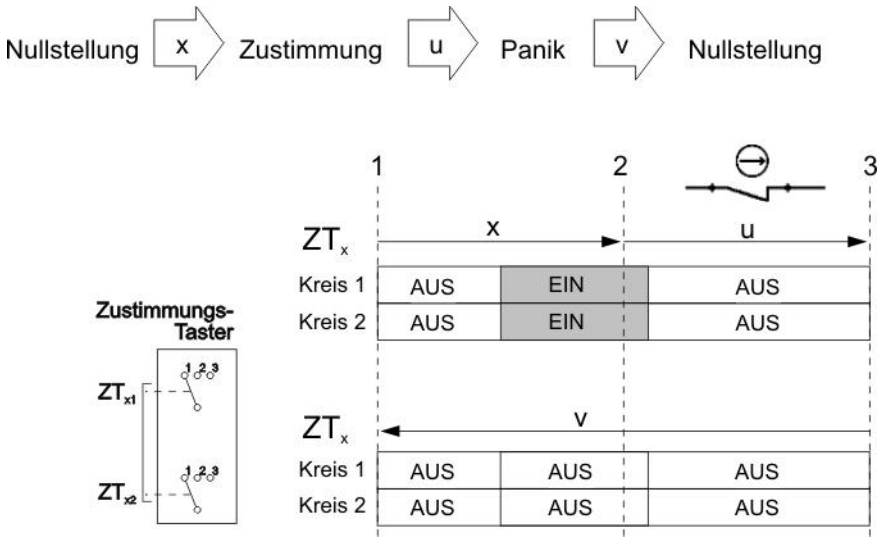


Abb. 4-19: Schaltwegediagramm für Panik-Betätigung

Information

Zustimmtaster sind beim KeTop immer 2-kreisig ausgeführt.

© KEBA 2021

Das Safe Wireless System erreicht Kategorie 4 PL e nach EN ISO 13849-1 und SIL3 nach EN 62061 / EN 61508.

4.6.5.3 Vorhersehbarer Missbrauch des Zustimmtasters

Ein unerlaubtes Fixieren der Zustimmtaster in der Zustimmstellung mit mechanischen Hilfsmitteln ist als vorhersehbarer Missbrauch anzusehen, welcher verhindert werden kann.

Das Handbediengerät hat hierfür folgende Maßnahmen integriert:

- Ist der Zustimmtaster bereits beim Einschalten des KeTop betätigt, so wird keine Zustimmung ausgegeben.
- Wird im Betrieb der Zustimmtaster länger als 15 Minuten in der Zustimmungsstellung gehalten, so wird die Zustimmung zurückgenommen, solange bis der Zustimmtaster losgelassen und erneut betätigt wird.

WARNUNG!

- Der Zustimmtaster ist als Schutzfunktion nur dann geeignet, wenn die den Zustimmtaster betätigende Person eine Personengefährdung rechtzeitig erkennt und dann sofort Maßnahmen zur Vermeidung von Gefahren treffen kann! Als Zusatzmaßnahme kann reduzierte Geschwindigkeit der Bewegung erforderlich sein. Die zulässige Geschwindigkeit muss anhand einer Risikobeurteilung ermittelt werden.
- Mit einem Zustimmtaster allein dürfen keine Befehle für gefahrbringende Zustände eingeleitet werden. Hierzu ist ein zweiter, bewusster Startbefehl erforderlich (Taste am Handbediengerät).
- Es darf sich nur jene Person im Gefahrenbereich aufhalten, die den Zustimmtaster betätigt.
- Für weitere Informationen zum Zustimmtaster ist unbedingt auch das Kapitel "Sicherheit von Maschinen" zu beachten.

4.6.6 USB-Port

Information

Die USB-Schnittstelle ist nicht als Betriebsschnittstelle für den laufenden Betrieb ausgelegt. Sie dient ausschließlich im Service- und Inbetriebnahmefall zum Anschluss von USB-Komponenten.

Anstecken einer USB-Komponente

Zum Anstecken gehen Sie wie folgt vor:

1) Aufklappen der Staubschutzklappe (optional).
2) USB-Komponente bis zum Einrasten einstecken.

Die USB-Komponente wird vom Betriebssystem erkannt und angezeigt.

© KEBA 2021

Abziehen einer USB-Komponente

Information

Falls ein Speichervorgang auf die USB-Komponente stattfindet, darf diese während des Speichervorgangs nicht abgezogen werden! Sonst kann es zu Datenverlust kommen.

Zum Abstecken gehen Sie wie folgt vor:

1) USB-Komponente abziehen.
2) Staubschutzklappe fest andrücken (optional).

KEBA © KEBA 2021

5 Basisstation CB41x

Die CB41x ist die Standard-Ausführung der Basisstation. Die CB41x darf nur in der Konfiguration mit KEBA Wireless Handbediengeräten mit beleuchtetem Not-Halt verwendet werden.

Als Sicherheitsfunktion steht ein Not-Halt auf der Basisstation zur Verfügung. Die Sicherheitselektronik der Not-Halt Brückung ist zweikreisig ausgeführt und ermöglicht eine Umsetzung bis zu Kategorie 4 PL e nach EN ISO 13849-1 bzw. SIL 3 nach EN 62061 / EN 61508.

Im Auslieferzustand ist die Rückwand der Basisstation nicht mit dem Rest der Box verschraubt. Als Zubehör existiert für die Basisstation eine Rückwand, welche ein rückseitiges Verdrahten ermöglicht (siehe 17.7 Rückwand für rückseitige Kabelmontage (nur für CB41x)).

5.1 Frontansicht

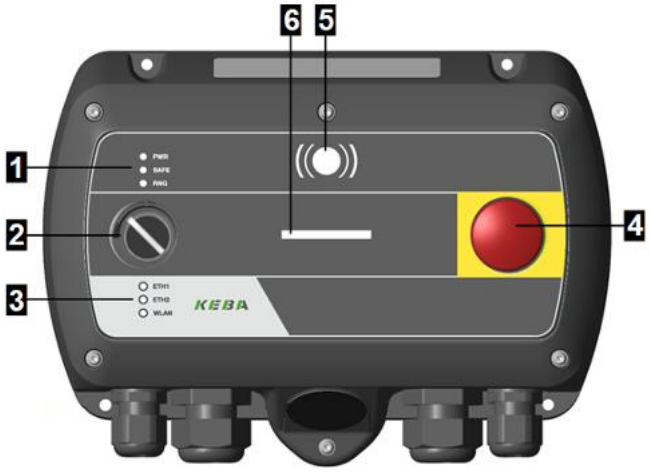


Abb. 5-20: Frontseite inklusive optionale Bedienelemente

1 ... Status LEDs (PWR, SAFE, RNG)	2 ... Direkt verdrahteter Schlüsselschalter (optional)
3 ... Verbindungs LEDs (ETH1, ETH2, WLAN)	4 ... Not-Halt
5 ... RFID Sensor	6 ... Status-LED-Balken

© KEBA 2021

5.2 Rückansicht

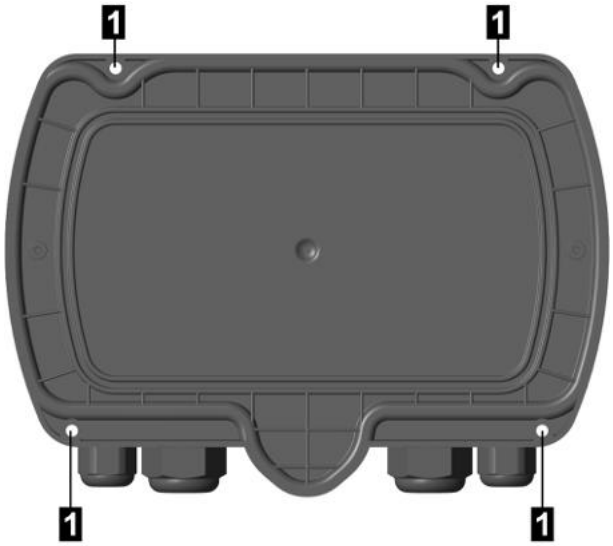


Abb. 5-21: Rückseite

1 ... Bohrlöcher	

5.3 Unterseite

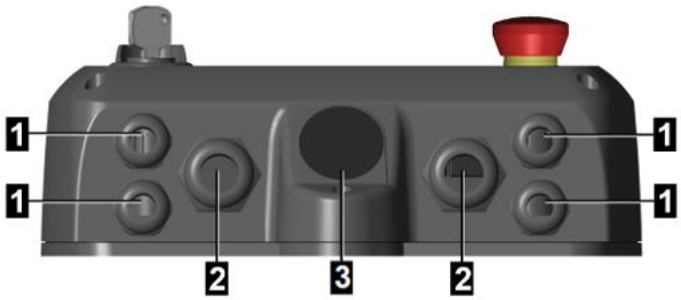


Abb. 5-22: Unterseite

1 ... Standard-Kabelauslässe	2 ... Ethernet-Kabelauslässe
3 ... "Pairing Reset" Schaltfläche (kapazitiv)	

KEBA © KEBA 2021

5.4 Oberseite

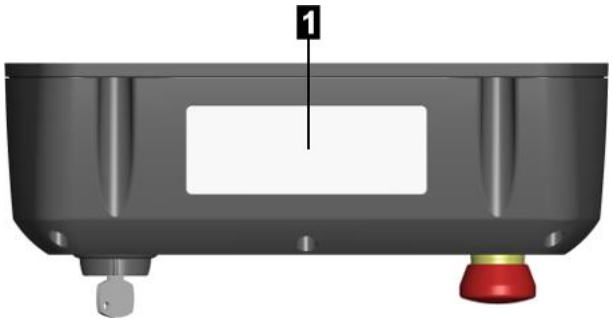


Abb. 5-23: Oberseite

1 ... Typenschild	

5.5 Typenschild

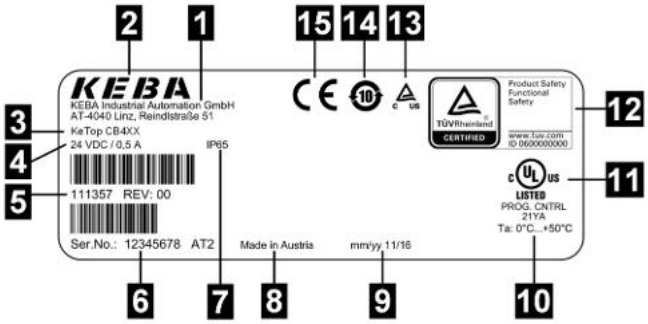


Abb. 5-24: Typenschild

1 ... Herstelleradresse	2 ... Hersteller
3 ... Produktbezeichnung	4 ... Technische Daten (Spannung / Strom)
5 ... Material- und Revisionsnummer	6 ... Seriennummer
7 ... Schutzart	8 ... Herstellungsland
9 ... Produktionsdatum	10 ... Umgebungstemperatur
11 ... UL-Prüfzeichen	12 ... TÜV-Prüfzeichen
13 ... cTÜVus-Prüfzeichen	14 ... China RoHS-Prüfzeichen
15 ... CE-Konformitätskennzeichnung	

5.6 Anzeigen und Bedienelemente

An der Frontseite der Baugruppe befinden sich zwei LED Gruppen und ein Status LED Balken.

© KEBA 2021

5.6.1 Status-LEDs

Die Basisstation ist mit folgenden LEDs bestückt:

PWR (Versorgungsspannung)

LED	Beschreibung
Dunkel	Keine Versorgungsspannung, Fehler beim Hochlauf
Grün	Versorgungsspannung vorhanden, Gerät betriebsbereit

SAFE (Sichere Verbindung)

LED	Beschreibung
Dunkel	Kein Handbediengerät mit der Basisstation verbunden
Grün	Handbediengerät dauerhaft verbunden ("gepairt")

Information

Eine leuchtende SAFE LED signalisiert, dass das Handbediengerät mit einer Basisstation sicher verbunden ("gepairt") ist, auch wenn keine aktive Funkverbindung besteht.

RNG (Bedienbereichsüberwachung)

LED	Beschreibung
Dunkel	Keine Bedienbereichsüberwachung konfiguriert oder verfügbar
Grün	Bedienbereichsüberwachung aktiv

5.6.2 Verbindungs LEDs

ETH1 / ETH2

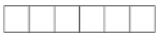
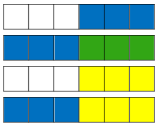
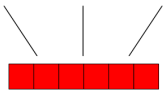
LED	Beschreibung
Dunkel	Keine Ethernet Verbindung verfügbar
Grün	Aktive Ethernet Verbindung (Datenübertragung)

WLAN

LED	Beschreibung
Dunkel	WLAN Modul nicht vorhanden oder nicht aktiv
Grün	WLAN Modul aktiv

KEBA © KEBA 2021

5.6.3 Status-LED-Balken

Anzeige Balken	Anzeige Signal-säule	Bedeutung
Grün	Grün	Betriebszustand "Normal" (siehe 9.3 Betriebszustände Basisstation)
Weiß 	Weiß	Betriebszustand "Bridge active" (siehe 9.3 Betriebszustände Basisstation)
Nacheinander erlöschende, gelbe LEDs	Gelb	Betriebszustand "Pairing/Unpairing timer" (siehe 9.3 Betriebszustände Basisstation)
Rot	Rot	Betriebszustand "Estop" (siehe 9.3 Betriebszustände Basisstation)
	Weiß und Blau Blau und Grün Weiß und Gelb Blau und Gelb	Sonderbetriebsart "Remote Paring" Diese Anzeigen werden wahlweise während eines Remote Pairing Vorgangs angezeigt und dienen der eindeutigen Identifikation der Basisstation.
Blau	Blau	Fehlerzustand (siehe 12 Diagnose)
Halb rot / halb blau	Rot und Blau	Fehlerzustand (siehe 12 Diagnose)
Halb gelb / halb rot blinken	Gelb und Rot	Fehlerzustand (siehe 12 Diagnose)
Rot blinken 	Rot und Weiß	Fehlerzustand (siehe 12 Diagnose)
Rotes Lauflicht	Rot	Fehlerzustand (siehe 12 Diagnose)

5.6.4 "Pairing Reset" Schaltfläche

Die "Pairing Reset" Schaltfläche dient dazu, das Handbediengerät manuell erzwungen abzumelden. Dazu muss die "Pairing Reset" Schaltfläche > 5 s gedrückt werden.

Diese Funktion wird benötigt, wenn ein reguläres Abmelden des Handbediengeräts an der Basisstation nicht mehr möglich ist (z.B. Defekt am Handbediengerät, Handbediengerät örtlich zu weit von der Basisstation entfernt, ...). Sie ist nur verfügbar, wenn die Basisstation keine Verbindung mehr zum Handbediengerät hat und sich im Zustand "Verbindungsabbruch" befindet.

© KEBA 2021

5.7 Montage- und Einbauhinweise

WARNUNG!

Die Basisstation darf nicht im Gefahrenbereich der Maschine montiert werden.

5.7.1 Positionierung der Basisstation

Die Basisstation ermöglicht dem Handbediengerät Zugriff auf das Funknetzwerk. Durch die richtige Positionierung der Basisstation kann ein möglichst störungsfreier Betrieb ermöglicht werden.

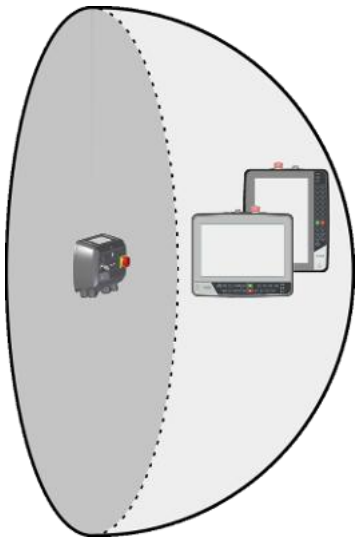


Abb. 5-25: Positionierung der Basisstation

Folgende Punkte sollten bei der Auswahl der Position der Basisstation beachtet werden:

- Die Basisstation muss in Sichtverbindung zum Bewegungsradius des Handbediengeräts aufgestellt werden. Der LED-Balken (oder die Signalsäule) muss aus dem Gefahrenbereich stets gut sichtbar sein.
- Die Basisstation sollte möglichst weg von großen metallischen Oberflächen, Glasflächen oder Wänden montiert werden.
- Die Basisstation muss in einem ungeschirmten Bereich montiert werden.
- Die Basisstationen selbst sollten möglichst weit voneinander entfernt montiert werden. Ein Mindestabstand von 2 m muss eingehalten werden.
- Der Abstand zum nächstgelegenen Zugriffspunkt einer WLAN-Verbindung ("Accesspoint") muss mind. 4 m betragen.

KEBA © KEBA 2021

- Der Mindestabstand der Basisstation zu Gegenständen oder baulichen Gegebenheiten beträgt nach oben und unten 1 m, rechts und links 0,5 m.
- Die Basisstation sollte mit dem Handbediengerät gut erreichbar sein, da der "Pairing"-Vorgang innerhalb einer Distanz von 0 - 2 m zwischen Basisstation und Handbediengerät erfolgen muss.

5.7.2 Bohrschablone für Wandmontage

Die Rückwand der Basisstation kann zum Anzeichnen der Bohrlöcher verwendet werden.

Das Schraubmaterial ist abhängig vom Baumaterial der Montageoberfläche, an der die Basisstation montiert werden soll.

Es wird empfohlen die Rückwand mit 4 Schrauben M4 mit einem maximalen Schraubenkopfdurchmesser von 9 mm zu montieren. Handelt es sich bei der Montageoberfläche z.B. um eine Schaltschrankwand wird empfohlen, die Schrauben fachgerecht und selbstsichernd zu montieren.

5.7.3 Montage der Basisstation

Gehäuse abnehmen

Für die Montage und Verdrahtung der Basisstation muss das Gehäuse von der Rückwand abgenommen werden. Hierfür müssen 6 PT30x10-Schrauben mit einem Torxschlüssel Größe 10 an der Vorderseite der Basisstation (siehe Abbildung) entfernt werden. Die entfernten Schrauben werden für den Zusammenbau wieder benötigt.

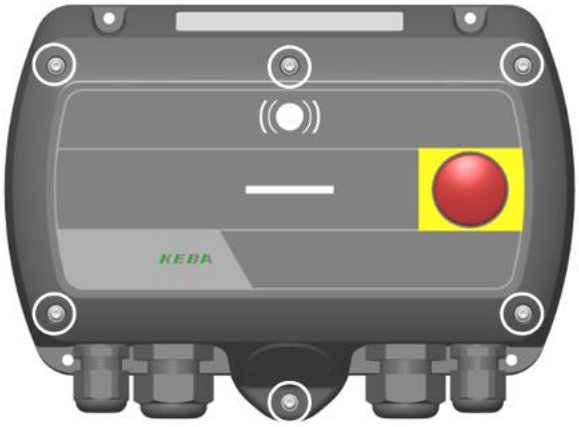


Abb. 5-26: Schrauben am Gehäuse

© KEBA 2021

Information

Die Basisstation ist zwischen Gehäuse und Rückwand bereits verkabelt. Für die anschließende Montage der Rückwand können die verbundenen Kabel vorübergehend abgesteckt werden (siehe 6.8.1 Interne Verkabelung).

Rückwand montieren

Information

Als Zubehör existiert für die Basisstation eine Rückwand, welche ein rückseitiges Verdrahten ermöglicht (siehe Rückwand für rückseitige Kabelmontage).

Um die Basisstation an der Montageoberfläche zu montieren, muss zuerst dessen Rückwand montiert werden. Gehen Sie dazu wie folgt vor:

1) Anzeichnen der Bohrlöcher mit Hilfe der Rückwand der Basisstation.
2) Bohren der Löcher.
3) Wenn nötig Dübel in die Löcher geben.
4) Rückwand, wie im folgenden Bild dargestellt, mittels geeigneter Schrauben an der Wand montieren.

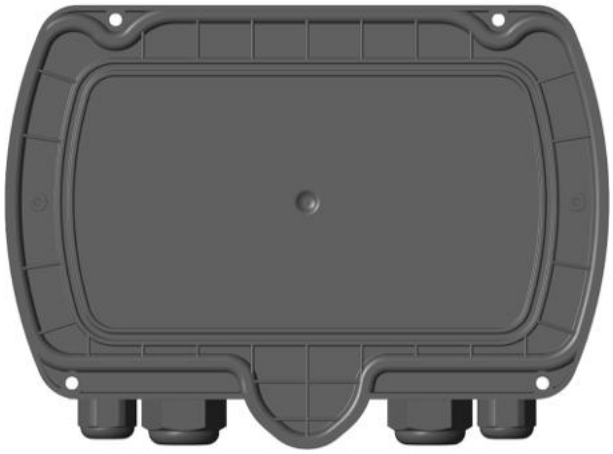


Abb. 5-27: Rückwand

Die Rückwand wurde montiert.

Danach kann die Verkabelung durchgeführt werden, bevor das Gehäuse geschlossen wird (siehe Anschlüsse und Verdrahtung).

KEBA © KEBA 2021

5.8 Anschlüsse und Verdrahtung

WARNUNG!

Fehlerhafte Sicherheitsfunktion!

Achten Sie darauf, dass keine Drahtstücke, Füllungen oder Späne ins Gerät fallen, wenn Sie Löcher bohren oder Drähte verbinden.

ESD

Beachten Sie die ESD-Hinweise aus dem Kap. 2.4 ESD-Hinweise.

Achtung

Die Verkabelung der CB4xx darf ausschließlich durch elektrotechnisch geschultes Fachpersonal und unter Beachtung der beschriebenen Hinweise erfolgen!

Folgende Anschlüsse sind verfügbar, wobei alle individuell über die Kabellauslässe nach außen geführt werden können.

Information

Steckstellen, die in der folgenden Abbildung nicht nummeriert sind, dürfen nicht verwendet werden.

Anschlüsse Basisstation CB410

Abb. 5-28: Anschlüsse der Basisstation CB410

1 ... Klemmleiste S1 / Spannungsversorgung	2 ... Ethernet-Schnittstellen

© KEBA 2021

3 ... DIP-Switch (Bedienbereichs-Konfiguration)	4 ... Klemmleiste "Pairing" / "Remote Pairing" Ausgänge, "Fast Response" Buttons (optional)
5 ... Klemmleiste "Fast Response" Buttons (optional)	6 ... Klemmleiste S2
7 ... Klemmleiste "Signal" für externe LED Anzeige	

Verkabelungshilfe

Um das Gerät zu verkabeln, kann es umgedreht an die montierte Rückwand gesteckt werden.

Dazu wird das Gehäuse frontseitig mit den oberen zwei Löcher zum Verschrauben auf die zwei längeren Befestigungsstifte der Rückwand gesteckt.

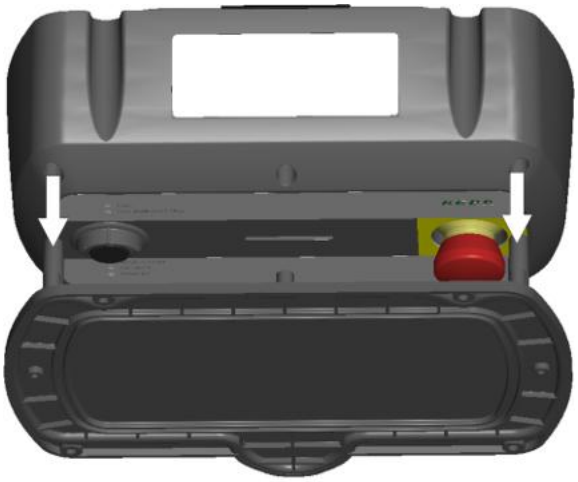


Abb. 5-29: Auf Rückwand aufstecken

Danach werden die Kabel durch die entsprechenden Kabelauslässe an der Unterseite des Geräts geführt. Diese besitzen folgende Spezifikationen:

Standard-Kabelauslässe

Klemmbereich (mögliche Kabeldurchmesser):	4 bis 8 mm
Schutzart:	IP68
Größe:	M16 x 1,5
Größe Gabelschlüssel:	SW19
Drehmoment beim Verschrauben:	3 Nm

Ethernet-Kabelauslässe

Klemmbereich (mögliche Kabeldurchmesser):	6 mm
Schutzart:	IP68
Größe:	M20 x 1,5
Max. Durchmesser RJ45-Stecker:	14,4 mm

KEBA © KEBA 2021

Größe Gabelschlüssel:	SW27 (Kappe), SW24 (Körper)
Drehmoment beim Verschrauben:	6 Nm

Um die Kabel durch die Kabelauslässe zu führen, muss zuerst die Verschraubung abgenommen und über das gewünschte Kabel geschoben werden. Bei den Ethernetkabeln muss zusätzlich der Dichtring, welcher sich im Kabelauslass befindet, um das Kabel gegeben werden.

Danach können die Kabel in das Gerät geführt, die Verschraubungen wieder handfest verschraubt und die Verkabelung durchgeführt werden.

Achtung

Nicht verwendete Kabelauslässe müssen mit den mitgelieferten Blindabdeckungen abgedichtet werden, um die Schutzart zu gewährleisten. Dazu werden die PG-Abdeckungen entfernt und die Blindabdeckungen mit folgenden Drehmomenten montiert (Kreuzschlitzgröße Z3):

- M16 × 1,5: 2 Nm
- M20 × 1,5: 2 Nm

Für die Verkabelung über die Rückseite steht als Zubehör eine spezielle Rückwand zur Verfügung (siehe 17.7 Rückwand für rückseitige Kabelmontage (nur für CB41x)).

5.8.1 Klemmleiste S1 / Spannungsversorgung

An der Klemme S1 wird die CB4xx mit Spannung versorgt. Weiters liegen die Signale des Zustimmtasters und des Not-Halts des Handbediengeräts an der Klemme.

WARNUNG!

Beachten Sie die sicherheitsrelevanten Hinweise im Kapitel 2.3 Sicherheitshinweise zur Personensicherheit.

Ist die Basisstation mit Spannung versorgt, leuchtet die PWR LED grün und der Balken leuchtet weiß (= die Not-Halt-Ausgänge der Basisstation sind geschlossen).

© KEBA 2021

5.8.1.1 Pinbelegung

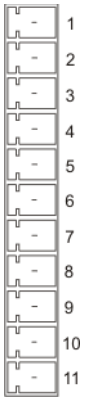


Abb. 5-30: Pinbelegung

Pin-Nr.	Signalbezeichnung	Beschreibung
1	N.C.	nicht verbunden
2	ZT2-	Freigabesteuerung, Kreis 2 neg.
3	ZT1-	Freigabesteuerung, Kreis 1 neg.
4	ZT2+	Freigabesteuerung, Kreis 2 pos.
5	ZT1+	Freigabesteuerung, Kreis 1 pos.
6	ES2	Not-Halt, Kreis 2
7	ES1	Not-Halt, Kreis 1
8	ES2	Not-Halt, Kreis 2
9	ES1	Not-Halt, Kreis 1
10	-	GND
11	+	24 V DC Spannungsversorgung

5.8.2 Klemmleiste S2

Die Klemmleiste S2 ist direkt verdrahtet und kann für Sicherheitsfunktionen verwendet werden.

Ist die Basisstation mit einem optionalen Schlüsselschalter ausgestattet, liegen an der Klemme S2 die Signale des Bedienelements an. Die Kombination der Pegel zweier Kontakte gibt die Position des Schlüsselschalters an (siehe 5.8.2.1 Pinbelegung).

KEBA © KEBA 2021

5.8.2.1 Pinbelegung

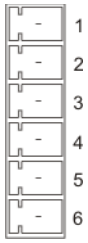
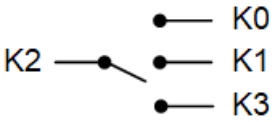


Abb. 5-31: Pinbelegung

Pin-Nr.	Signalbezeichnung	Beschreibung
1	GND	Erdung
2	n.a.	Keine Verwendung möglich
3	K3	Schlüsselschalterkontakt: Position 3 (rechte Schaltstellung) 
4	K2	Schlüsselschalterkontakt: COMMON
5	K1	Schlüsselschalterkontakt: Position 2 (mittlere Schaltstellung)
6	K0	Schlüsselschalterkontakt: Position 1 (linke Schaltstellung)

5.8.3 Klemmleiste "Signal"

An der Klemme "Signal" kann eine Signalsäule angeschlossen werden.

Die Basisstation wurde von KEBA mit folgenden Signalsäulen getestet:

Hersteller	Produktbezeichnung
PATLITE	LR4-_02LJN
SPÄLTI	MES-502A-RYGBC(DC24V)

Die Verwendung dieser Signalsäulen wird empfohlen. Weitere Informationen siehe Dokumentation des Herstellers.

Information

Die Klemmleiste "Signal" darf nur zum Anschluss einer Signalsäule für die Anzeige der Betriebs- und Diagnosezustände der Basisstation genutzt werden.

© KEBA 2021

5.8.3.1 Pinbelegung

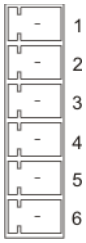


Abb. 5-32: Pinbelegung

Pin-Nr.	Signalbezeichnung	Beschreibung
1	24V	Spannungsversorgung 24 V DC
2	WH	Signalfarbe Transparent/Weiß
3	BU	Signalfarbe Blau
4	Y/O	Signalfarbe Gelb
5	GN	Signalfarbe Grün
6	RD	Signalfarbe Rot

5.8.4 Klemmleiste "Pairing" / "Remote Pairing" Ausgänge

Über die kombinierte Verwendung und Plausibilisierung des "Pairing" Statusausgangs und des "Remote Pairing" Statusausgangs über eine externe Sicherheitssteuerung kann eine sichere Betriebsartenumschaltung realisiert werden. (Weitere Informationen siehe 11 Verbinden mit Basisstation.)

Mögliche Zustände

PA1	PA2	Beschreibung
0 (offen)	0 (offen)	Kein Gerät verbunden
1 (geschlossen)	0 (offen)	Gerät wurde über "Pairing" verbunden
0 (offen)	1 (geschlossen)	Gerät wurde über "Remote Pairing" verbunden
1 (geschlossen)	1 (geschlossen)	Ein Defekt liegt vor

KEBA © KEBA 2021

5.8.4.1 Pinbelegung

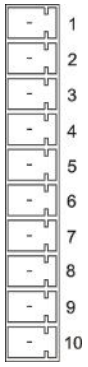


Abb. 5-33: Pinbelegung

Pin-Nr.	Signalbezeich-nung	Beschreibung
1	PA1	Pairingausgang
2	PA2	Remote Pairingausgang
3	PA1	Pairingausgang
4	PA2	Remote Pairingausgang

5.8.5 Klemmleisten Fast Response Buttons

Mit den funktionalen Fast Response Buttons können Tasten des Handbediengeräts direkt mit den Ausgängen der Basisstation verknüpft werden. Ein Tastendruck am Handbediengerät wird sofort auf den verknüpften Ausgang der Basisstation angelegt. Dadurch ergibt sich eine kürzere Reaktionszeit. (Konfiguration siehe 8.4.1 Basestation.)

5.8.5.1 Pinbelegung

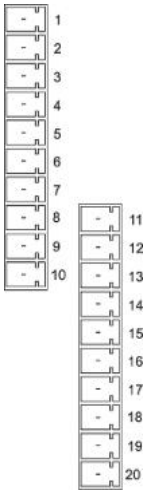


Abb. 5-34: Pinbelegung

© KEBA 2021

Pin-Nr.	Signalbezeich-nung	Beschreibung
5	GND	Ground
6	14	D14
7	13	D13
8	12	D12
9	11	D11
10	10	D10

Pin-Nr.	Signalbezeich-nung	Beschreibung
11	GND	Ground
12	09	D9
13	08	D8
14	07	D7
15	06	D6
16	05	D5
17	04	D4
18	03	D3
19	02	D2
20	01	D1

5.8.6 Ethernet

Das Gerät stellt 2 Ethernet-Schnittstellen zur Verfügung. Diese dienen zum Anschluss von Geräten, mit denen das Handbediengerät kommunizieren soll. Die Schnittstellen können über die Kabelausgänge nach außen geführt werden.

5.8.6.1 Pinbelegung

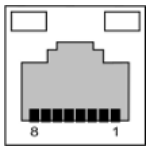


Abb. 5-35: RJ45 Buchse

Pin-Nr.	Signalbezeichnung		Eingang/Ausgang
1	Tr. Data+	Transmit Data +	Ausgang
2	Tr. Data-	Transmit Data -	Ausgang
3	Re. Data+	Receive Data +	Eingang
4	n.c.	n.c.	---
5	n.c.	n.c.	---

KEBA © KEBA 2021

Pin-Nr.	Signalbezeichnung		Eingang/Ausgang
6	Re. Data-	Receive Data -	Eingang
7	n.c.	n.c.	---
8	n.c.	n.c.	---

5.8.7 Änderungen an der Verkabelung

Information

Informationen zu Änderungen an der Verkabelung:

- Beim Abstecken von Steckverbindungen ist darauf zu achten, dass der Stecker durch Ziehen mit den Fingern an seinen Adern abgesteckt wird (keine spitzen Gegenstände dafür zu Hilfe nehmen).
- Beim Abstecken der RJ45-Stecker ist darauf zu achten, dass der Verriegelungshebel dabei betätigt wird:

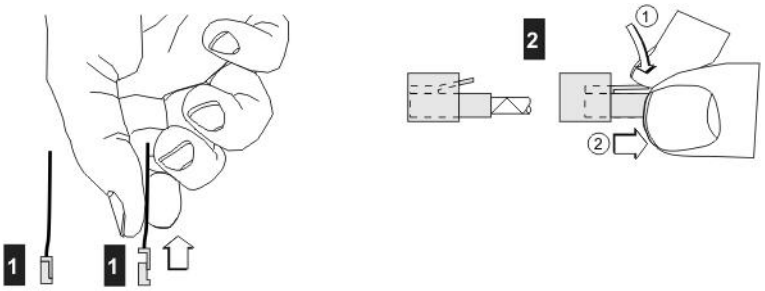


Abb. 5-36: Abstecken des Hauptsteckers und des RJ-45-Steckers

1 ... Hauptstecker	2 ... RJ45-Stecker

5.8.8 Schließen der Basisstation

Um die Basisstation zu schließen, wird das Gehäuse von der Rückwand abgenommen und umgedreht. Danach kann das Gehäuse an der Rückwand aufgelegt und mittels 6 PT30x10-Schrauben (benötigtes Werkzeug - Torx Größe 10), wie in der Abbildung gezeigt, verschraubt werden. Die Schrauben sind im Lieferumfang enthalten.

© KEBA 2021

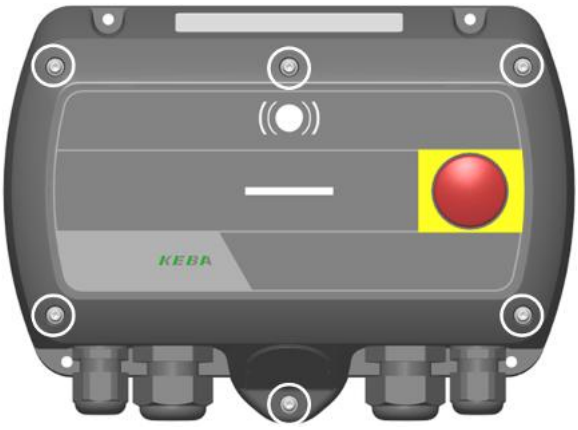


Abb. 5-37: Schrauben für den Zusammenbau

Information

Informationen zum Schließen der Basisstation:

- Die Dichtung muss sauber und unbeschädigt sein und sich an der richtigen Position befinden.
- Es dürfen keine Kabel eingeklemmt werden.
- Die Basisstation muss mit allen PT30x10-Schrauben wieder verschraubt werden (Drehmoment: 0,85 Nm - 1,15 Nm). Nur dadurch kann die entsprechende Schutzart gewährleistet werden.

Die Basisstation ist betriebsbereit.

5.8.9 Not-Halt

Die Basisstation ist mit einem Not-Halt ausgestattet.

WARNUNG!

Nicht funktionstüchtige Not-Halt-Einrichtungen können fatale Folgen haben! Rot-gelb gekennzeichnete Not-Halt müssen jederzeit und in allen Betriebsarten einer Maschine oder Anlage wirksam sein.

WARNUNG!

Der Not-Halt am nicht verbundenen Handbediengerät ist kein Ersatz für den Not-Halt auf der Maschine. Es muss immer ein stationär fest verdrahteter Not-Halt an der Maschine verfügbar sein.

KEBA © KEBA 2021

5.8.10 Anschlussbeispiel für die Zustimmfunktion mit Überwachungsgerät (PILZ PNOZ s3)

WARNUNG!

Für die Erkennung von Kurz- und Querschlüssen in der Anschlussleitung muss ein geeignetes Überwachungsgerät eingesetzt werden.

Das folgende Beispiel soll als Hilfestellung zur Realisierung in der Endapplikation dienen:

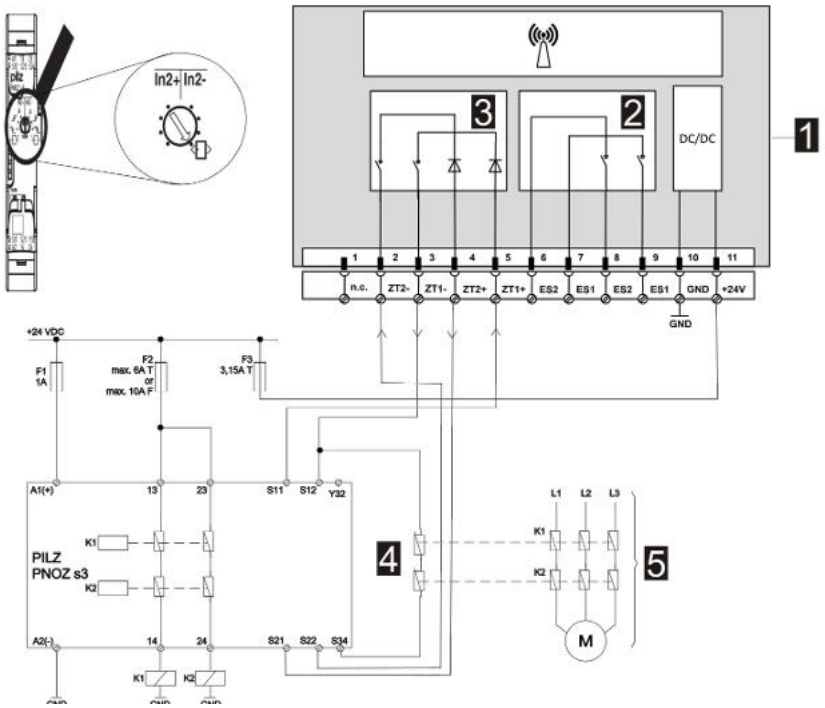


Abb. 5-38: Anschlussbeispiel für KeTop an PILZ PNOZ s3 Überwachungsgerät

1 ... Basisstation	2 ... Not-Halt
3 ... Zustimmtaster	4 ... Startbedingung mit Kontrollüberwachung
5 ... Freigabe der gefährlichen Bewegung!	

Die Grafik zeigt einen Schaltungsvorschlag zur Erreichung der Kategorie 4 PL e für die Zustimmfunktion mit PILZ-Überwachungsgerät. Es ist die Betriebsanleitung der Fa. PILZ zum Gerät PNOZ s3 zusätzlich zu beachten. Für die Berechnung der gesamten Sicherheitsfunktion "Freigabe über Zustimmtaster" sind das Überwachungsgerät und nachfolgende Komponenten noch mit zu berücksichtigen.

Klemmenbelegung S1 siehe 5.8.1.1 Pinbelegung.

© KEBA 2021

5.8.11 Anschlussbeispiel für Zustimmfunktion und Not-Halt mit KEBA Sicherheitssteuerung

Bei Verwendung der Sicherheitssteuerung von KEBA (D3-DU 3x5/x) kann zusätzlich zum Zustimmtaster auch der Not-Halt an dieser angeschlossen werden.

Das folgende Beispiel soll als Hilfestellung zur Realisierung in der Endapplikation dienen:

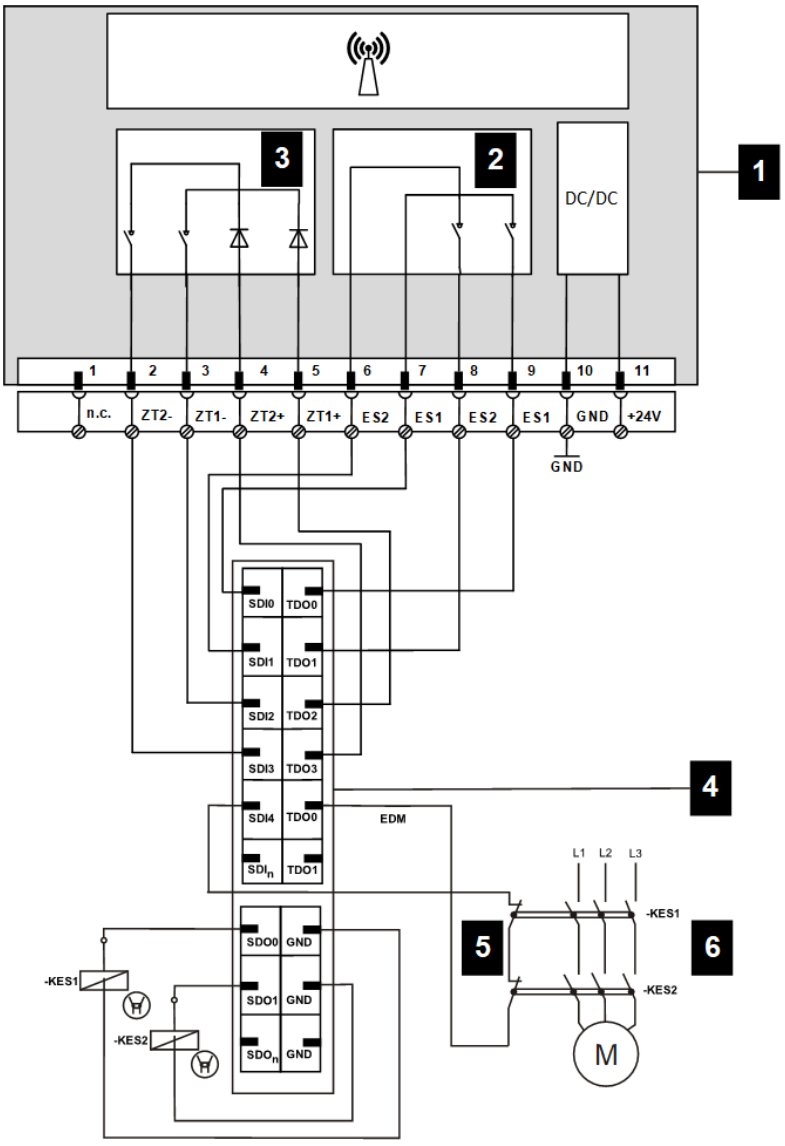


Abb. 5-39: Anschlussbeispiel mit KEBA Sicherheitssteuerung (ein Zustimmtaster)

1 ... Basisstation	2 ... Not-Halt
3 ... Zustimmtaster	4 ... Sicherheitssteuerung
5 ... EDM (External Device Monitoring)	6 ... Freigabe der gefährlichen Bewegung!

© KEBA 2021

Die Grafik zeigt einen Schaltungsvorschlag für den Zustimmtaster und dem Not-Halt mit der Sicherheitssteuerung von KEBA.

© KEBA 2021

6 Basisstation CB42x

Die CB42x verfügt als Basisstation über ein zusätzliches PROFINET / PROFIsafe-Gateway. Die CB42x darf nur in der Konfiguration mit KEBA Wireless Handbediengeräten mit beleuchtetem Not-Halt verwendet werden.

Die Basisstation ist auch als Variante CB421 mit zusätzlichem Kabeldurchlass an der Rückseite verfügbar.

Als Sicherheitsfunktion steht ein Not-Halt auf der Basisstation zur Verfügung. Die Sicherheitselektronik der Not-Halt Brückung ist zweikreisig ausgeführt und ermöglicht eine Umsetzung bis zu Kategorie 4 PL e nach EN ISO 13849-1 bzw. SIL 3 nach EN 62061 / EN 61508.

6.1 Frontansicht

Abb. 6-40: Frontansicht

1 ... Status LEDs (PWR, SAFE, RNG)	2 ... Verbindungs LEDs (ETH1,ETH2, WLAN)
3 ... Not-Halt	4 ... RFID Sensor
5 ... Status-LED-Balken	

KEBA © KEBA 2021

6.2 Rückansicht

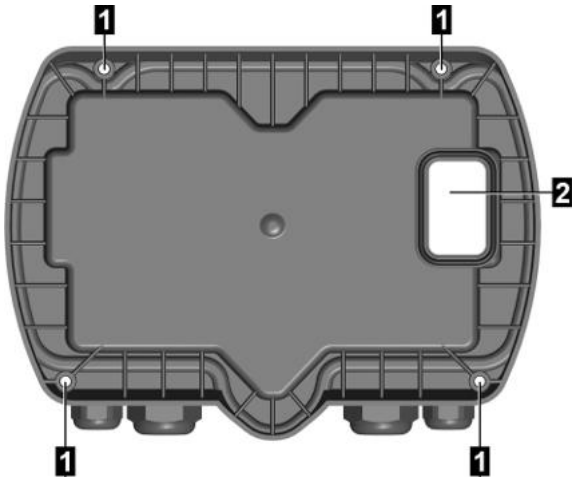


Abb. 6-41: Rückansicht

1 ... Bohrlöcher	2 ... Kabeldurchlass (nur bei CB421)

6.3 Unterseite

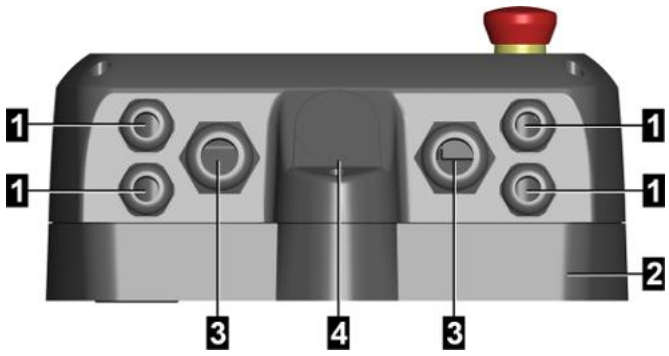


Abb. 6-42: Unterseite

1 ... Standard-Kabelauslässe	2 ... PROFINET / PROFIsafe-Gateway
3 ... Ethernet-Kabelauslässe	4 ... "Pairing Reset" Schaltfläche (kapazitiv)

© KEBA 2021

6.4 Oberseite

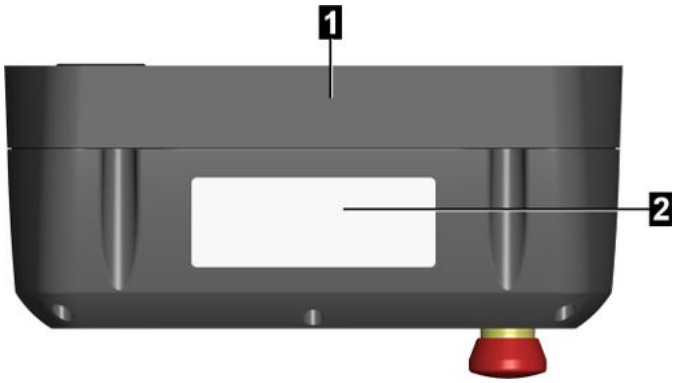


Abb. 6-43: Oberseite

1 ... PROFINET / PROFIsafe-Gateway	2 ... Typenschild

6.5 Typenschild

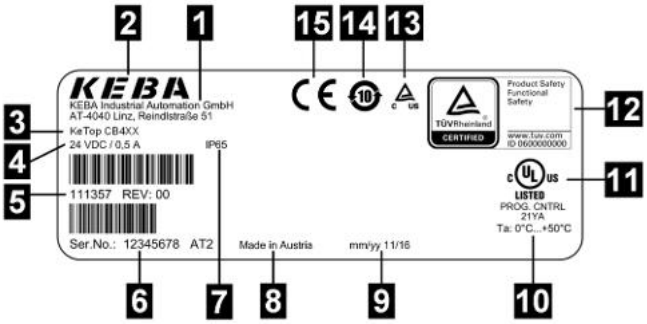


Abb. 6-44: Typenschild

1 ... Herstelleradresse	2 ... Hersteller
3 ... Produktbezeichnung	4 ... Technische Daten (Spannung / Strom)
5 ... Material- und Revisionsnummer	6 ... Seriennummer
7 ... Schutzart	8 ... Herstellungsland
9 ... Produktionsdatum	10 ... Umgebungstemperatur
11 ... UL-Prüfzeichen	12 ... TÜV-Prüfzeichen
13 ... cTÜVus-Prüfzeichen	14 ... China RoHS-Prüfzeichen
15 ... CE-Konformitätskennzeichnung	

6.6 Anzeigen und Bedienelemente

An der Frontseite der Baugruppe befinden sich zwei LED Gruppen und ein Status LED Balken.

KEBA © KEBA 2021

6.6.1 Status-LEDs

Die Basisstation ist mit folgenden LEDs bestückt:

PWR (Versorgungsspannung)

LED	Beschreibung
Dunkel	Keine Versorgungsspannung, Fehler beim Hochlauf
Grün	Versorgungsspannung vorhanden, Gerät betriebsbereit

SAFE (Sichere Verbindung)

LED	Beschreibung
Dunkel	Kein Handbediengerät mit der Basisstation verbunden
Grün	Handbediengerät dauerhaft verbunden ("gepairt")
Grün blinkend	PROFINET SF/DCP

Information

Eine leuchtende SAFE LED signalisiert, dass das Handbediengerät mit einer Basisstation sicher verbunden ("gepairt") ist, auch wenn keine aktive Funkverbindung besteht.

RNG (Bedienbereichsüberwachung)

LED	Beschreibung
Dunkel	Keine Bedienbereichsüberwachung konfiguriert oder verfügbar
Grün	Bedienbereichsüberwachung aktiv

6.6.2 Verbindungs LEDs

ETH1 / ETH2

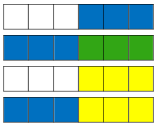
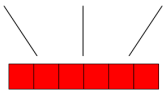
LED	Beschreibung
Dunkel	Keine Ethernet Verbindung verfügbar
Grün	Aktive Ethernet Verbindung (Datenübertragung)

WLAN

LED	Beschreibung
Dunkel	WLAN Modul nicht vorhanden oder nicht aktiv
Grün	WLAN Modul aktiv

© KEBA 2021

6.6.3 Status-LED-Balken

Anzeige Balken	Anzeige Signal-säule	Bedeutung
Grün	Grün	Betriebszustand "Normal" (siehe 9.3 Betriebszustände Basisstation)
Weiß	Weiß	Betriebszustand "Bridge active" (siehe 9.3 Betriebszustände Basisstation)
Nacheinander erlöschende, gelbe LEDs	Gelb	Betriebszustand "Pairing/Unpairing timer" (siehe 9.3 Betriebszustände Basisstation)
Rot	Rot	Betriebszustand "Estop" (siehe 9.3 Betriebszustände Basisstation)
Gelb	Gelb	Betriebsart "Stop" Keine sichere Verbindung zur Sicherheitssteuerung aufgebaut.
Gelb blinken	Gelb und Weiß	Betriebszustand "Standby" Feldbus-Verbindung ist aufgebaut und sicherer Zustand wird signalisiert. Kein Austausch sicherer Prozessdaten. Anwender-Quittung notwendig.
	Weiß und Blau Blau und Grün Weiß und Gelb Blau und Gelb	Sonderbetriebsart "Remote Paring" Diese Anzeigen werden wahlweise während eines Remote Pairing Vorgangs angezeigt und dienen der eindeutigen Identifikation der Basisstation.
Blau	Blau	Fehlerzustand (siehe 12 Diagnose)
Halb rot / halb blau	Rot und Blau	Fehlerzustand (siehe 12 Diagnose)
Halb gelb / halb rot blinken	Gelb und Rot	Fehlerzustand (siehe 12 Diagnose)
Rot blinken 	Rot und Weiß	Fehlerzustand (siehe 12 Diagnose)
Rotes Lauflicht	Rot	Fehlerzustand (siehe 12 Diagnose)

6.6.4 "Pairing Reset" Schaltfläche

Die "Pairing Reset" Schaltfläche dient dazu, das Handbediengerät manuell erzwungen abzumelden. Dazu muss die "Pairing Reset" Schaltfläche > 5 s gedrückt werden.

KEBA © KEBA 2021

Diese Funktion wird benötigt, wenn ein reguläres Abmelden des Handbediengeräts an der Basisstation nicht mehr möglich ist (z.B. Defekt am Handbediengerät, Handbediengerät örtlich zu weit von der Basisstation entfernt, ...). Sie ist nur verfügbar, wenn die Basisstation keine Verbindung mehr zum Handbediengerät hat und sich im Zustand "Verbindungsabbruch" befindet.

6.7 Montage- und Einbauhinweise

WARNUNG!

Die Basisstation darf nicht im Gefahrenbereich der Maschine montiert werden.

6.7.1 Positionierung der Basisstation

Die Basisstation ermöglicht dem Handbediengerät Zugriff auf das Funknetzwerk. Durch die richtige Positionierung der Basisstation kann ein möglichst störungsfreier Betrieb ermöglicht werden.

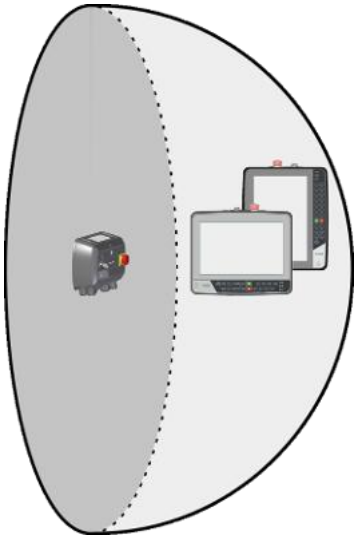


Abb. 6-45: Positionierung der Basisstation

Folgende Punkte sollten bei der Auswahl der Position der Basisstation beachtet werden:

- Die Basisstation muss in Sichtverbindung zum Bewegungsradius des Handbediengeräts aufgestellt werden. Der LED-Balken (oder die Signalsäule) muss aus dem Gefahrenbereich stets gut sichtbar sein.
- Die Basisstation sollte möglichst weg von großen metallischen Oberflächen, Glasflächen oder Wänden montiert werden.
- Die Basisstation muss in einem ungeschirmten Bereich montiert werden.

© KEBA 2021

- Die Basisstationen selbst sollten möglichst weit voneinander entfernt montiert werden. Ein Mindestabstand von 2 m muss eingehalten werden.
- Der Abstand zum nächstgelegenen Zugriffspunkt einer WLAN-Verbindung ("Accesspoint") muss mind. 4 m betragen.
- Der Mindestabstand der Basisstation zu Gegenständen oder baulichen Gegebenheiten beträgt nach oben und unten 1 m, rechts und links 0,5 m.
- Die Basisstation sollte mit dem Handbediengerät gut erreichbar sein, da der "Pairing"-Vorgang innerhalb einer Distanz von 0 - 2 m zwischen Basisstation und Handbediengerät erfolgen muss.

6.7.2 Bohrschablone für Wandmontage

Die Rückwand der Basisstation kann zum Anzeichnen der Bohrlöcher verwendet werden.

Das Schraubmaterial ist abhängig vom Baumaterial der Montageoberfläche, an der die Basisstation montiert werden soll.

Es wird empfohlen die Rückwand mit 4 Schrauben M4 mit einem maximalen Schraubenkopfdurchmesser von 9 mm zu montieren. Handelt es sich bei der Montageoberfläche z.B. um eine Schaltschrankwand wird empfohlen, die Schrauben fachgerecht und selbstsichernd zu montieren.

6.7.3 Montage der Basisstation

Gehäuse abnehmen

Für die Montage und Verdrahtung der Basisstation muss das Gehäuse von der Rückwand abgenommen werden. Hierfür müssen 6 PT30x10-Schrauben mit einem Torxschlüssel Größe 10 an der Vorderseite der Basisstation (siehe Abbildung) entfernt werden. Die entfernten Schrauben werden für den Zusammenbau wieder benötigt.

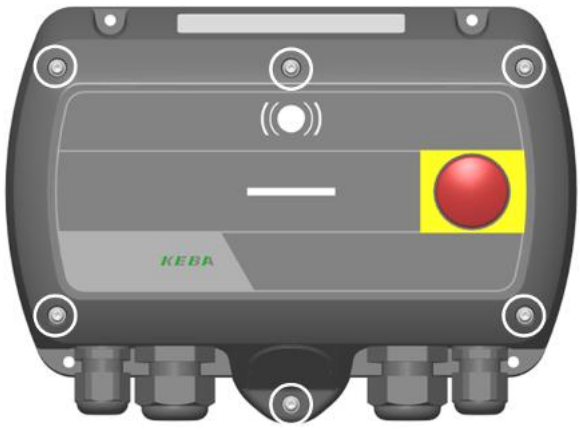


Abb. 6-46: Schrauben am Gehäuse

KEBA © KEBA 2021

Information

Die Basisstation ist zwischen Gehäuse und Rückwand bereits verkabelt. Für die anschließende Montage der Rückwand können die verbundenen Kabel vorübergehend abgesteckt werden (siehe 6.8.1 Interne Verkabelung).

Rückwand montieren

Information

Als Zubehör existiert für die Basisstation eine Rückwand, welche ein rückseitiges Verdrahten ermöglicht (siehe Rückwand für rückseitige Kabelmontage).

Um die Basisstation an der Montageoberfläche zu montieren, muss zuerst dessen Rückwand montiert werden. Gehen Sie dazu wie folgt vor:

1) Anzeichnen der Bohrlöcher mit Hilfe der Rückwand der Basisstation.
2) Bohren der Löcher.
3) Wenn nötig Dübel in die Löcher geben.
4) Rückwand, wie im folgenden Bild dargestellt, mittels geeigneter Schrauben an der Wand montieren.

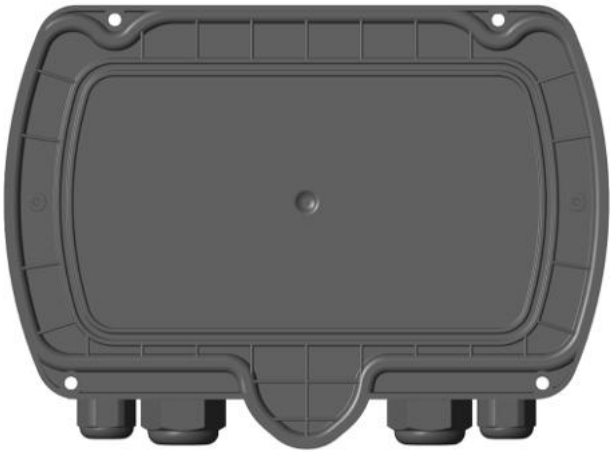


Abb. 6-47: Rückwand

Die Rückwand wurde montiert.

Danach kann die Verkabelung durchgeführt werden, bevor das Gehäuse geschlossen wird (siehe Anschlüsse und Verdrahtung).

© KEBA 2021

6.8 Anschlüsse und Verdrahtung

WARNUNG!

Fehlerhafte Sicherheitsfunktion!

Achten Sie darauf, dass keine Drahtstücke, Füllungen oder Späne ins Gerät fallen, wenn Sie Löcher bohren oder Drähte verbinden.

ESD

Beachten Sie die ESD-Hinweise aus dem Kap. 2.4 ESD-Hinweise.

Achtung

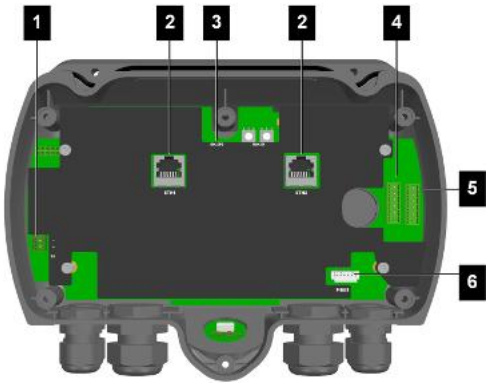
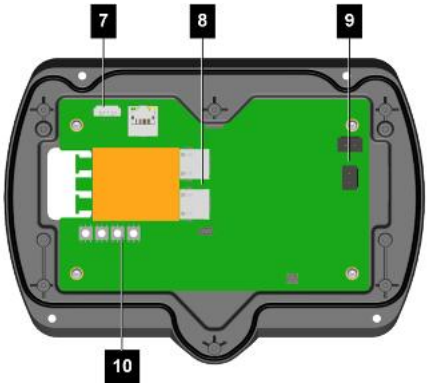
Die Verkabelung der CB4xx darf ausschließlich durch elektrotechnisch geschultes Fachpersonal und unter Beachtung der beschriebenen Hinweise erfolgen!

Folgende Anschlüsse sind verfügbar, wobei alle individuell über die Kabellauslässe nach außen geführt werden können.

Information

Steckstellen, die in der folgenden Abbildung nicht nummeriert sind, dürfen nicht verwendet werden.

Anschlüsse Basisstation CB42x mit PROFINET / PROFIsafe-Gateway

CB42x	PROFINET / PROFIsafe-Gateway
	

1	Klemmleiste S1 / Spannungsversorgung	2	Ethernet-Schnittstellen
3	DIP-Switch (Bedienbereichs-Konfiguration)	4	Klemmleiste S2
5	Klemmleiste "Signal" für externe LED-Anzeige	6	Interface PROFINET / PROFIsafe-Gateway
7	Interface CB42x	8	PROFINET-Schnittstellen

KEBA © KEBA 2021

9	Anschluss Spannungsversorgung (VIN)	10	F-Adressschalter

Verkabelungshilfe

Um das Gerät zu verkabeln, kann es umgedreht an die montierte Rückwand gesteckt werden.

Dazu wird das Gehäuse frontseitig mit den oberen zwei Löcher zum Verschrauben auf die zwei längeren Befestigungsstifte der Rückwand gesteckt.

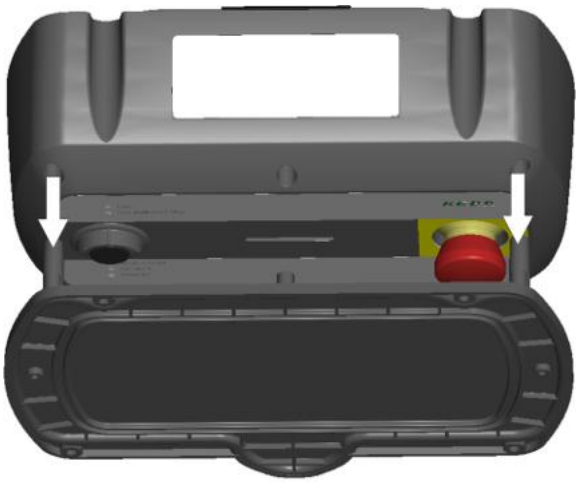


Abb. 6-48: Auf Rückwand aufstecken

Danach werden die Kabel durch die entsprechenden Kabelauslässe an der Unterseite des Geräts geführt. Diese besitzen folgende Spezifikationen:

Standard-Kabelauslässe

Klemmbereich (mögliche Kabeldurchmesser):	4 bis 8 mm
Schutzart:	IP68
Größe:	M16 x 1,5
Größe Gabelschlüssel:	SW19
Drehmoment beim Verschrauben:	3 Nm

Ethernet-Kabelauslässe

Klemmbereich (mögliche Kabeldurchmesser):	6 mm
Schutzart:	IP68
Größe:	M20 x 1,5
Max. Durchmesser RJ45-Stecker:	14,4 mm
Größe Gabelschlüssel:	SW27 (Kappe), SW24 (Körper)
Drehmoment beim Verschrauben:	6 Nm

© KEBA 2021

Um die Kabel durch die Kabelauslässe zu führen, muss zuerst die Verschraubung abgenommen und über das gewünschte Kabel geschoben werden. Bei den Ethernetkabeln muss zusätzlich der Dichtring, welcher sich im Kabelauslass befindet, um das Kabel gegeben werden.

Danach können die Kabel in das Gerät geführt, die Verschraubungen wieder handfest verschraubt und die Verkabelung durchgeführt werden.

Achtung

Nicht verwendete Kabelauslässe müssen mit den mitgelieferten Blindabdeckungen abgedichtet werden, um die Schutzart zu gewährleisten. Dazu werden die PG-Abdeckungen entfernt und die Blindabdeckungen mit folgenden Drehmomenten montiert (Kreuzschlitzgröße Z3):

- M16 × 1,5: 2 Nm
- M20 × 1,5: 2 Nm

6.8.1 Interne Verkabelung

Für die interne Spannungsversorgung und Datenübertragung zwischen CB42x und PROFINET / PROFIsafe-Gateway sind bereits folgende Anschlüsse miteinander verbunden:

Spannungsversorgung

- Anschluss Gateway: VIN Stecker - CB42x: Klemmleiste S1 (siehe 6.8.2.1 Pinbelegung)

Datenübertragung

- Anschluss Gateway: Interface CB42x - CB42x: Interface PROFINET / PROFIsafe-Gateway

6.8.2 Klemmleiste S1 / Spannungsversorgung

Bei der CB42x ist die Klemmleiste S1 2-polig ausgeführt. Die Spannungsversorgung erfolgt mittels VOUT-Stecker am PROFINET / PROFIsafe-Gateway und wird von dort zur Klemme S1 geführt.

WARNUNG!

Beachten Sie die sicherheitsrelevanten Hinweise im Kapitel 2.3 Sicherheitshinweise zur Personensicherheit.

Ist die Basisstation mit Spannung versorgt, leuchtet die PWR LED grün und der Balken leuchtet weiß (= die Not-Halt-Ausgänge der Basisstation sind geschlossen).

KEBA © KEBA 2021

6.8.2.1 Pinbelegung

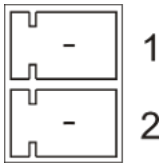


Abb. 6-49: Pinbelegung

Pin-Nr.	Signalbezeichnung	Beschreibung
1	-	GND
2	+	24 V DC Spannungsversorgung

6.8.3 Klemmleiste S2

Die Klemmleiste S2 ist direkt verdrahtet und kann für Sicherheitsfunktionen verwendet werden.

Ist die Basisstation mit einem optionalen Schlüsselschalter ausgestattet, liegen an der Klemme S2 die Signale des Bedienelements an. Die Kombination der Pegel zweier Kontakte gibt die Position des Schlüsselschalters an (siehe 6.8.3.1 Pinbelegung).

6.8.3.1 Pinbelegung

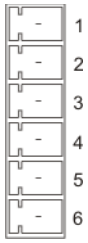
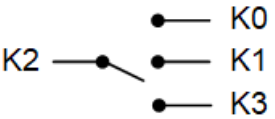


Abb. 6-50: Pinbelegung

Pin-Nr.	Signalbezeichnung	Beschreibung
1	GND	Erdung
2	n.a.	Keine Verwendung möglich
3	K3	Schlüsselschalterkontakt: Position 3 (rechte Schaltstellung) 
4	K2	Schlüsselschalterkontakt: COMMON
5	K1	Schlüsselschalterkontakt: Position 2 (mittlere Schaltstellung)

© KEBA 2021

Pin-Nr.	Signalbezeichnung	Beschreibung
6	K0	Schlüsselschalterkontakt: Position 1 (linke Schaltstellung)

6.8.4 Klemmleiste "Signal"

An der Klemme "Signal" kann eine Signalsäule angeschlossen werden.

Die Basisstation wurde von KEBA mit folgenden Signalsäulen getestet:

Hersteller	Produktbezeichnung
PATLITE	LR4-_02LJN
SPÄLTI	MES-502A-RYGBC(DC24V)

Die Verwendung dieser Signalsäulen wird empfohlen. Weitere Informationen siehe Dokumentation des Herstellers.

Information

Die Klemmleiste "Signal" darf nur zum Anschluss einer Signalsäule für die Anzeige der Betriebs- und Diagnosezustände der Basisstation genutzt werden.

6.8.4.1 Pinbelegung

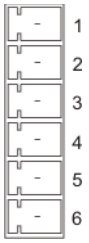


Abb. 6-51: Pinbelegung

Pin-Nr.	Signalbezeichnung	Beschreibung
1	24V	Spannungsversorgung 24 V DC
2	WH	Signalfarbe Transparent/Weiß
3	BU	Signalfarbe Blau
4	Y/O	Signalfarbe Gelb
5	GN	Signalfarbe Grün
6	RD	Signalfarbe Rot

© KEBA 2021

6.8.5 Ethernet

Das Gerät stellt 2 Ethernet-Schnittstellen zur Verfügung. Diese dienen zum Anschluss von Geräten, mit denen das Handbediengerät kommunizieren soll. Die Schnittstellen können über die Kabelausgänge nach außen geführt werden.

6.8.5.1 Pinbelegung

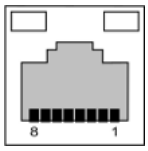


Abb. 6-52: RJ45 Buchse

Pin-Nr.	Signalbezeichnung		Eingang/Ausgang
1	Tr. Data+	Transmit Data +	Ausgang
2	Tr. Data-	Transmit Data -	Ausgang
3	Re. Data+	Receive Data +	Eingang
4	n.c.	n.c.	---
5	n.c.	n.c.	---
6	Re. Data-	Receive Data -	Eingang
7	n.c.	n.c.	---
8	n.c.	n.c.	---

6.8.6 PROFINET

Das Gatewaymodul besitzt 2 PROFINET-Schnittstellen. Die Schnittstellen können über die Kabelausgänge am CB42x oder durch die Öffnung (optional) an der Rückseite des PROFINET / PROFIsafe-Gateways nach außen geführt werden.

Folgende Steckverbinder können verwendet werden:

Hersteller	Produktbezeichnung
Siemens	6GK1901-1BB10-2AA0 (FastConnect)
Weidmüller	IE-PS-RJ45-FH-BK

Achtung

An den Laschen des Prints muss mit Kabelbindern eine Zugentlastung der angeschlossenen Kabel durchgeführt werden!

© KEBA 2021

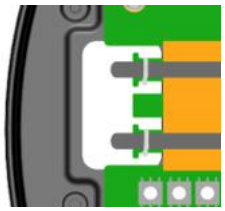


Abb. 6-53: Beispiel: Zwei angeschlossene Kabel mit Kabelbindern als Zugentlastung

6.8.7 Änderungen an der Verkabelung

Information

Informationen zu Änderungen an der Verkabelung:

- Beim Abstecken von Steckverbindungen ist darauf zu achten, dass der Stecker durch Ziehen mit den Fingern an seinen Adern abgesteckt wird (keine spitzen Gegenstände dafür zu Hilfe nehmen).
- Beim Abstecken der RJ45-Stecker ist darauf zu achten, dass der Verriegelungshebel dabei betätigt wird:

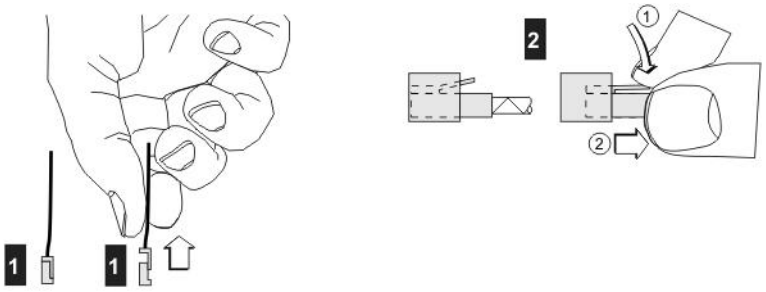


Abb. 6-54: Abstecken des Hauptsteckers und des RJ-45-Steckers

1 ... Hauptstecker	2 ... RJ45-Stecker

6.8.8 Schließen der Basisstation

Um die Basisstation zu schließen, wird das Gehäuse von der Rückwand abgenommen und umgedreht. Danach kann das Gehäuse an der Rückwand aufgelegt und mittels 6 PT30x10-Schrauben (benötigtes Werkzeug - Torx Größe 10), wie in der Abbildung gezeigt, verschraubt werden. Die Schrauben sind im Lieferumfang enthalten.

KEBA © KEBA 2021

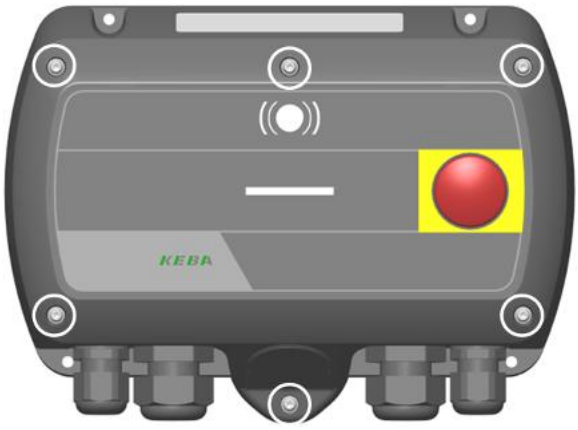


Abb. 6-55: Schrauben für den Zusammenbau

Information

Informationen zum Schließen der Basisstation:

- Die Dichtung muss sauber und unbeschädigt sein und sich an der richtigen Position befinden.
- Es dürfen keine Kabel eingeklemmt werden.
- Die Basisstation muss mit allen PT30x10-Schrauben wieder verschraubt werden (Drehmoment: 0,85 Nm - 1,15 Nm). Nur dadurch kann die entsprechende Schutzart gewährleistet werden.

Die Basisstation ist betriebsbereit.

6.8.9 Not-Halt

Die Basisstation ist mit einem Not-Halt ausgestattet.

WARNUNG!

Nicht funktionstüchtige Not-Halt-Einrichtungen können fatale Folgen haben! Rot-gelb gekennzeichnete Not-Halt müssen jederzeit und in allen Betriebsarten einer Maschine oder Anlage wirksam sein.

WARNUNG!

Der Not-Halt am nicht verbundenen Handbediengerät ist kein Ersatz für den Not-Halt auf der Maschine. Es muss immer ein stationär fest verdrahteter Not-Halt an der Maschine verfügbar sein.

© KEBA 2021

6.9 Fehlerquittierung

WARNUNG!

Lebensgefahr durch unerwartetes Anfahren der Maschine

Bei einer automatischen Wiedereingliederung, z.B. nach einem Busfehler, wird die CB4xx wieder in den vorherigen Zustand versetzt. Ohne übergeordnete, sichere Maßnahme kann die Maschine wieder anfahren und zu schweren Verletzungen oder Tod führen.

- Sicherstellen, dass die verwendete Sicherheitssteuerung keine automatische Wiedereingliederung des F-Devices vornimmt.

Alle Fehler, die lokal im Wirelesssystem auftreten, müssen an der CB4xx oder am Handbediengerät quittiert werden. Diese Fehler werden an der CB4xx mit einem rot/gelben LED Balken signalisiert.

Eine Quittierung erfolgt durch das Drücken/Entriegeln des Nothalts. Die erfolgte Quittierung wird an der CB4xx durch einen gelb blinkenden LED-Balken signalisiert. Erst danach ist eine softwareseitige Quittierung am F-Host durch das Setzen einer Anwenderquittierung möglich.

KEBA © KEBA 2021

7 Basisstation CB43x

Die CB43x verfügt als Basisstation über ein zusätzliches EtherCAT / FSoE-Gateway. Die CB43x darf nur in der Konfiguration mit KEBA Wireless Handbediengeräten mit beleuchtetem Not-Halt verwendet werden.

Die Basisstation ist auch als Variante CB431 mit zusätzlichem Kabeldurchlass an der Rückseite verfügbar.

Als Sicherheitsfunktion steht ein Not-Halt auf der Basisstation zur Verfügung. Die Sicherheitselektronik der Not-Halt Brückung ist zweikreisig ausgeführt und ermöglicht eine Umsetzung bis zu Kategorie 4 PL e nach EN ISO 13849-1 bzw. SIL 3 nach EN 62061 / EN 61508.

7.1 Frontansicht

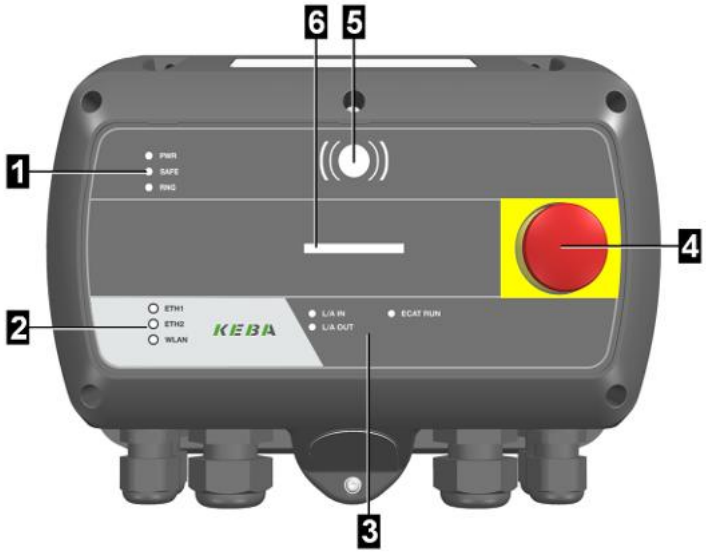


Abb. 7-56: Frontansicht

1 ... Status LEDs (PWR, SAFE, RNG)	2 ... Verbindungs-LEDs (ETH1, ETH2, WLAN)
3 ... EtherCAT-LEDs	4 ... Not-Halt
5 ... RFID Sensor	6 ... Status-LED-Balken

© KEBA 2021

7.2 Rückansicht

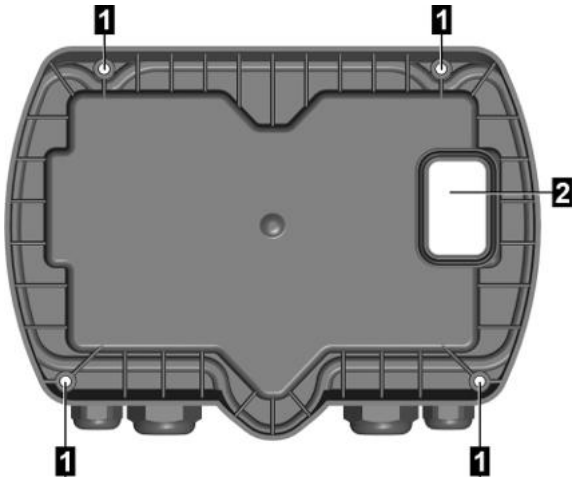


Abb. 7-57: Rückansicht

1 ... Bohrlöcher	2 ... Kabeldurchlass (nur bei CB431)

7.3 Unterseite

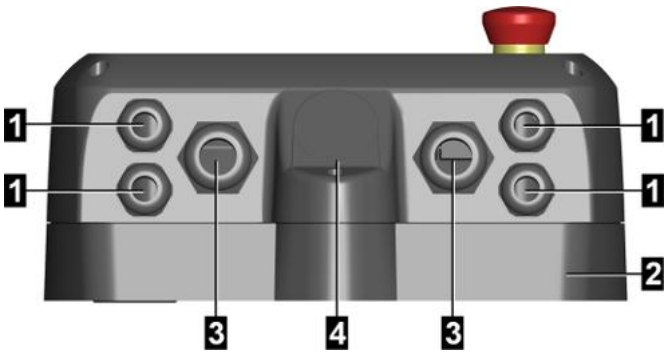


Abb. 7-58: Unterseite

1 ... Standard-Kabelauslässe	2 ... EtherCAT / FSoE-Gateway
3 ... Ethernet-Kabelauslässe	4 ... "Pairing Reset" Schaltfläche (kapazitiv)

KEBA © KEBA 2021

7.4 Oberseite

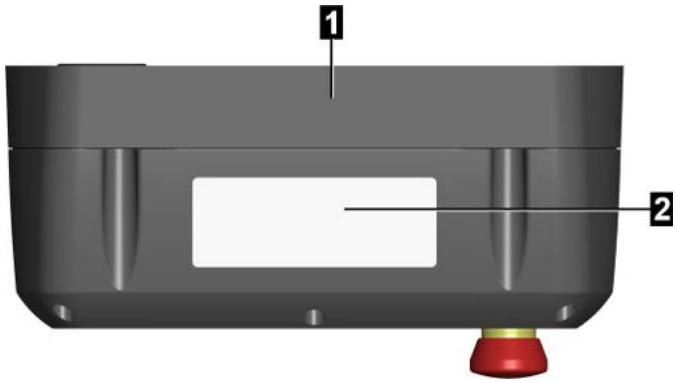


Abb. 7-59: Oberseite

1 ... EtherCAT / FSoE-Gateway	2 ... Typenschild

7.5 Typenschild

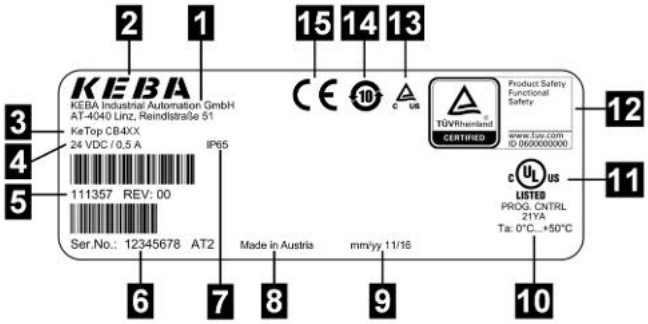


Abb. 7-60: Typenschild

1 ... Herstelleradresse	2 ... Hersteller
3 ... Produktbezeichnung	4 ... Technische Daten (Spannung / Strom)
5 ... Material- und Revisionsnummer	6 ... Seriennummer
7 ... Schutzart	8 ... Herstellungsland
9 ... Produktionsdatum	10 ... Umgebungstemperatur
11 ... UL-Prüfzeichen	12 ... TÜV-Prüfzeichen
13 ... cTÜVus-Prüfzeichen	14 ... China RoHS-Prüfzeichen
15 ... CE-Konformitätskennzeichnung	

7.6 Anzeigen und Bedienelemente

An der Frontseite der Baugruppe befinden sich zwei LED Gruppen und ein Status LED Balken.

© KEBA 2021

7.6.1 Status-LEDs

Die Basisstation ist mit folgenden LEDs bestückt:

PWR (Versorgungsspannung)

LED	Beschreibung
Dunkel	Keine Versorgungsspannung, Fehler beim Hochlauf
Grün	Versorgungsspannung vorhanden, Gerät betriebsbereit

SAFE (Sichere Verbindung)

LED	Beschreibung
Dunkel	Kein Handbediengerät mit der Basisstation verbunden
Grün	Handbediengerät dauerhaft verbunden ("gepairt")

Information

Eine leuchtende SAFE LED signalisiert, dass das Handbediengerät mit einer Basisstation sicher verbunden ("gepairt") ist, auch wenn keine aktive Funkverbindung besteht.

RNG (Bedienbereichsüberwachung)

LED	Beschreibung
Dunkel	Keine Bedienbereichsüberwachung konfiguriert oder verfügbar
Grün	Bedienbereichsüberwachung aktiv

7.6.2 Verbindungs LEDs

ETH1 / ETH2

LED	Beschreibung
Dunkel	Keine Ethernet Verbindung verfügbar
Grün	Aktive Ethernet Verbindung (Datenübertragung)

WLAN

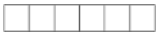
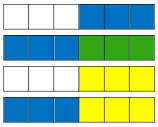
LED	Beschreibung
Dunkel	WLAN Modul nicht vorhanden oder nicht aktiv
Grün	WLAN Modul aktiv

KEBA © KEBA 2021

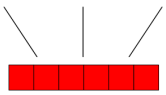
EtherCAT

LED	Beschreibung
L/A IN	
• Dunkel	Kein Link aufgebaut
• Grün blinken	Gerät empfängt Ethernet-Frames
• Grün	Link aufgebaut
L/A OUT	
• Dunkel	Kein Link aufgebaut
• Grün blinken	Gerät sendet Ethernet-Frames
• Grün	Link aufgebaut
ECAT RUN	
• Dunkel	Betriebszustand "INIT"
• Grün blinken	Betriebszustand "PRE-OPERATIONAL"
• Grün kurz blinken (200 ms ein, 1000 ms aus)	Betriebszustand "SAFE-OPERATIONAL"
• Grün	Betriebszustand "OPERATIONAL"

7.6.3 Status-LED-Balken

Anzeige Balken	Anzeige Signal-säule	Bedeutung
Grün	Grün	Betriebszustand "Normal" (siehe 9.3 Betriebszustände Basisstation)
Weiß 	Weiß	Betriebszustand "Bridge active" (siehe 9.3 Betriebszustände Basisstation)
Nacheinander erlöschende, gelbe LEDs	Gelb	Betriebszustand "Pairing/Unpairing timer" (siehe 9.3 Betriebszustände Basisstation)
Rot	Rot	Betriebszustand "Estop" (siehe 9.3 Betriebszustände Basisstation)
Gelb	Gelb	Betriebsart "Stop" Keine sichere Verbindung zur Sicherheitssteuerung aufgebaut.
Gelb blinken	Gelb und Weiß	Betriebszustand "Standby" Feldbus-Verbindung ist aufgebaut und sicherer Zustand wird signalisiert. Kein Austausch sicherer Prozessdaten. Anwender-Quittung notwendig.
	Weiß und Blau Blau und Grün Weiß und Gelb Blau und Gelb	Sonderbetriebsart "Remote Paring" Diese Anzeigen werden wahlweise während eines Remote Pairing Vorgangs angezeigt und dienen der eindeutigen Identifikation der Basisstation.

© KEBA 2021

Anzeige Balken	Anzeige Signal-säule	Bedeutung
Blau	Blau	Fehlerzustand (siehe 12 Diagnose)
Halb rot / halb blau	Rot und Blau	Fehlerzustand (siehe 12 Diagnose)
Halb gelb / halb rot blinken	Gelb und Rot	Fehlerzustand (siehe 12 Diagnose)
Rot blinken 	Rot und Weiß	Fehlerzustand (siehe 12 Diagnose)
Rotes Lauflicht	Rot	Fehlerzustand (siehe 12 Diagnose)

7.6.4 "Pairing Reset" Schaltfläche

Die "Pairing Reset" Schaltfläche dient dazu, das Handbediengerät manuell erzwungen abzumelden. Dazu muss die "Pairing Reset" Schaltfläche > 5 s gedrückt werden.

Diese Funktion wird benötigt, wenn ein reguläres Abmelden des Handbediengeräts an der Basisstation nicht mehr möglich ist (z.B. Defekt am Handbediengerät, Handbediengerät örtlich zu weit von der Basisstation entfernt, ...). Sie ist nur verfügbar, wenn die Basisstation keine Verbindung mehr zum Handbediengerät hat und sich im Zustand "Verbindungsabbruch" befindet.

7.7 Montage- und Einbauhinweise

WARNUNG!

Die Basisstation darf nicht im Gefahrenbereich der Maschine montiert werden.

7.7.1 Positionierung der Basisstation

Die Basisstation ermöglicht dem Handbediengerät Zugriff auf das Funknetzwerk. Durch die richtige Positionierung der Basisstation kann ein möglichst störungsfreier Betrieb ermöglicht werden.

KEBA © KEBA 2021

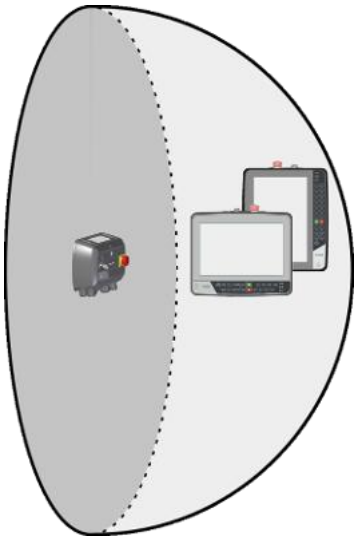


Abb. 7-61: Positionierung der Basisstation

Folgende Punkte sollten bei der Auswahl der Position der Basisstation beachtet werden:

- Die Basisstation muss in Sichtverbindung zum Bewegungsradius des Handbediengeräts aufgestellt werden. Der LED-Balken (oder die Signalsäule) muss aus dem Gefahrenbereich stets gut sichtbar sein.
- Die Basisstation sollte möglichst weg von großen metallischen Oberflächen, Glasflächen oder Wänden montiert werden.
- Die Basisstation muss in einem ungeschirmten Bereich montiert werden.
- Die Basisstationen selbst sollten möglichst weit voneinander entfernt montiert werden. Ein Mindestabstand von 2 m muss eingehalten werden.
- Der Abstand zum nächstgelegenen Zugriffspunkt einer WLAN-Verbindung ("Accesspoint") muss mind. 4 m betragen.
- Der Mindestabstand der Basisstation zu Gegenständen oder baulichen Gegebenheiten beträgt nach oben und unten 1 m, rechts und links 0,5 m.
- Die Basisstation sollte mit dem Handbediengerät gut erreichbar sein, da der "Pairing"-Vorgang innerhalb einer Distanz von 0 - 2 m zwischen Basisstation und Handbediengerät erfolgen muss.

7.7.2 Bohrschablone für Wandmontage

Die Rückwand der Basisstation kann zum Anzeichnen der Bohrlöcher verwendet werden.

Das Schraubmaterial ist abhängig vom Baumaterial der Montageoberfläche, an der die Basisstation montiert werden soll.

© KEBA 2021

Es wird empfohlen die Rückwand mit 4 Schrauben M4 mit einem maximalen Schraubenkopfdurchmesser von 9 mm zu montieren. Handelt es sich bei der Montageoberfläche z.B. um eine Schaltschrankwand wird empfohlen, die Schrauben fachgerecht und selbstsichernd zu montieren.

7.7.3 Montage der Basisstation

Gehäuse abnehmen

Für die Montage und Verdrahtung der Basisstation muss das Gehäuse von der Rückwand abgenommen werden. Hierfür müssen 6 PT30x10-Schrauben mit einem Torxschlüssel Größe 10 an der Vorderseite der Basisstation (siehe Abbildung) entfernt werden. Die entfernten Schrauben werden für den Zusammenbau wieder benötigt.

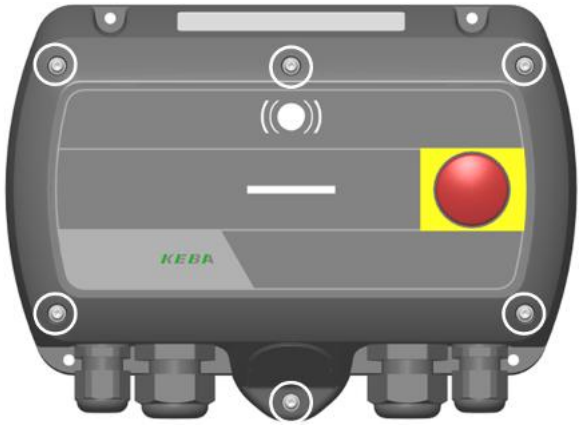


Abb. 7-62: Schrauben am Gehäuse

Information

Die Basisstation ist zwischen Gehäuse und Rückwand bereits verkabelt. Für die anschließende Montage der Rückwand können die verbundenen Kabel vorübergehend abgesteckt werden (siehe 6.8.1 Interne Verkabelung).

Rückwand montieren

Information

Als Zubehör existiert für die Basisstation eine Rückwand, welche ein rückseitiges Verdrahten ermöglicht (siehe Rückwand für rückseitige Kabelmontage).

Um die Basisstation an der Montageoberfläche zu montieren, muss zuerst dessen Rückwand montiert werden. Gehen Sie dazu wie folgt vor:

1) Anzeichnen der Bohrlöcher mit Hilfe der Rückwand der Basisstation.
2) Bohren der Löcher.

KEBA © KEBA 2021

3) Wenn nötig Dübel in die Löcher geben.

4) Rückwand, wie im folgenden Bild dargestellt, mittels geeigneter Schrauben an der Wand montieren.

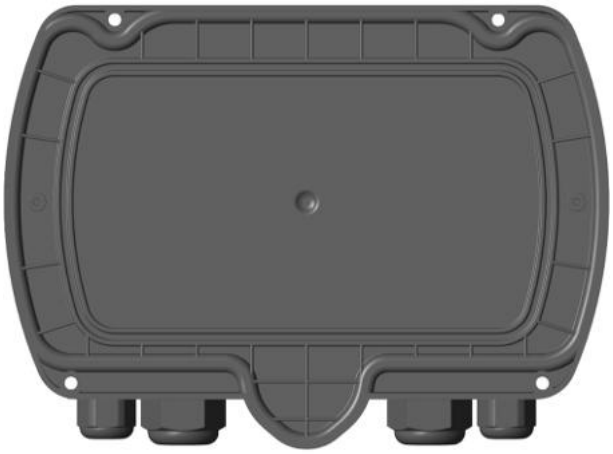


Abb. 7-63: Rückwand

Die Rückwand wurde montiert.

Danach kann die Verkabelung durchgeführt werden, bevor das Gehäuse geschlossen wird (siehe Anschlüsse und Verdrahtung).

7.8 Anschlüsse und Verdrahtung

WARNUNG!

Fehlerhafte Sicherheitsfunktion!

Achten Sie darauf, dass keine Drahtstücke, Füllungen oder Späne ins Gerät fallen, wenn Sie Löcher bohren oder Drähte verbinden.

ESD

Beachten Sie die ESD-Hinweise aus dem Kap. 2.4 ESD-Hinweise.

Achtung

Die Verkabelung der CB4xx darf ausschließlich durch elektrotechnisch geschultes Fachpersonal und unter Beachtung der beschriebenen Hinweise erfolgen!

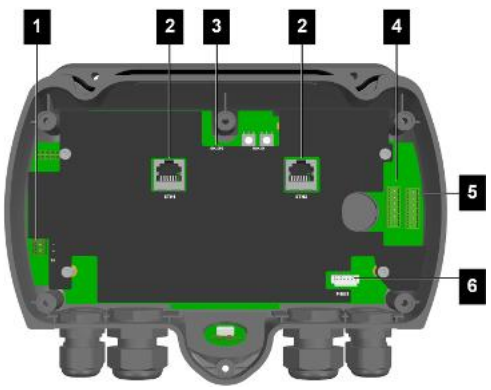
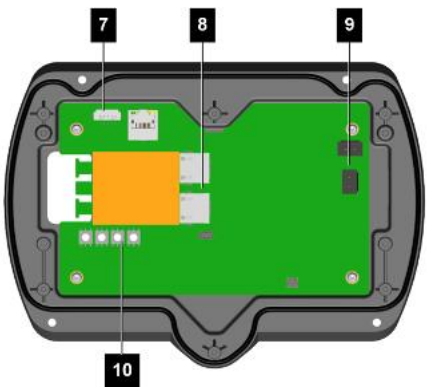
Folgende Anschlüsse sind verfügbar, wobei alle individuell über die Kabellauslässe nach außen geführt werden können.

© KEBA 2021

Information

Steckstellen, die in der folgenden Abbildung nicht nummeriert sind, dürfen nicht verwendet werden.

Anschlüsse Basisstation CB43x mit EtherCAT / FSoE-Gateway

CB43x	EtherCAT / FSoE-Gateway
	

1	Klemmleiste S1 / Spannungsversor-gung	2	Ethernet-Schnittstellen
3	DIP-Switch (Bedienbereichs-Konfigu-ration)	4	Klemmleiste S2
5	Klemmleiste "Signal" für externe LED-Anzeige	6	Interface EtherCAT / FSoE-Gateway
7	Interface CB43x	8	EtherCAT-Schnittstellen
9	Anschluss Spannungsversorgung (VIN)	10	F-Adressschalter

Eine der beiden EtherCAT-Schnittstellen wird für die Verbindung zum Ether-CAT- oder FSoE-Master verwendet. Die zweite Schnittstelle ermöglicht den Anschluss weiterer EtherCAT-Geräte in Reihen- oder Baumtopologien

Verkabelungshilfe

Um das Gerät zu verkabeln, kann es umgedreht an die montierte Rückwand gesteckt werden.

Dazu wird das Gehäuse frontseitig mit den oberen zwei Löcher zum Ver-schrauben auf die zwei längeren Befestigungsstifte der Rückwand gesteckt.

KEBA © KEBA 2021

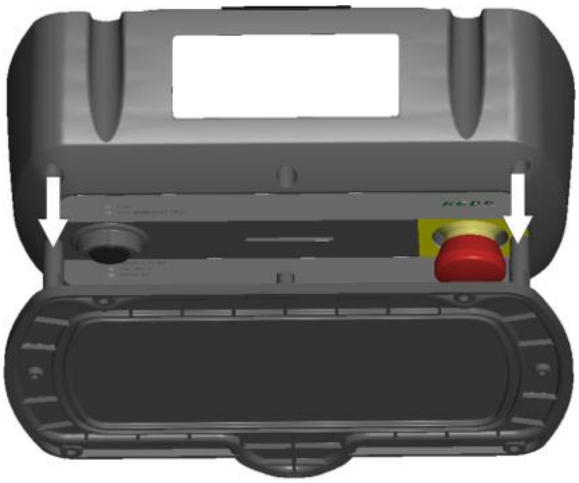


Abb. 7-64: Auf Rückwand aufstecken

Danach werden die Kabel durch die entsprechenden Kabelauslässe an der Unterseite des Geräts geführt. Diese besitzen folgende Spezifikationen:

Standard-Kabelauslässe

Klemmbereich (mögliche Kabeldurchmesser):	4 bis 8 mm
Schutzart:	IP68
Größe:	M16 x 1,5
Größe Gabelschlüssel:	SW19
Drehmoment beim Verschrauben:	3 Nm

Ethernet-Kabelauslässe

Klemmbereich (mögliche Kabeldurchmesser):	6 mm
Schutzart:	IP68
Größe:	M20 x 1,5
Max. Durchmesser RJ45-Stecker:	14,4 mm
Größe Gabelschlüssel:	SW27 (Kappe), SW24 (Körper)
Drehmoment beim Verschrauben:	6 Nm

Um die Kabel durch die Kabelauslässe zu führen, muss zuerst die Verschraubung abgenommen und über das gewünschte Kabel geschoben werden. Bei den Ethernetkabeln muss zusätzlich der Dichtring, welcher sich im Kabelauslass befindet, um das Kabel gegeben werden.

Danach können die Kabel in das Gerät geführt, die Verschraubungen wieder handfest verschraubt und die Verkabelung durchgeführt werden.

© KEBA 2021

Achtung

Nicht verwendete Kabelauslässe müssen mit den mitgelieferten Blindabdeckungen abgedichtet werden, um die Schutzart zu gewährleisten. Dazu werden die PG-Abdeckungen entfernt und die Blindabdeckungen mit folgenden Drehmomenten montiert (Kreuzschlitzgröße Z3):

- M16 × 1,5: 2 Nm
- M20 × 1,5: 2 Nm

7.8.1 Interne Verkabelung

Für die interne Spannungsversorgung und Datenübertragung zwischen CB43x und EtherCAT / FSoE-Gateway sind bereits folgende Anschlüsse miteinander verbunden:

Spannungsversorgung

- Anschluss Gateway: VIN Stecker - CB43x: Klemmleiste S1 (siehe 7.8.2.1 Pinbelegung)

Datenübertragung

- Anschluss Gateway: Interface CB43x - CB43x: Interface EtherCAT / FSoE-Gateway

7.8.2 Klemmleiste S1 / Spannungsversorgung

Bei der CB43x ist die Klemmleiste S1 2-polig ausgeführt. Die Spannungsversorgung erfolgt mittels VOUT-Stecker am EtherCAT/FSoE-Gateway und wird von dort zur Klemme S1 geführt.

WARNUNG!

Beachten Sie die sicherheitsrelevanten Hinweise im Kapitel 2.3 Sicherheitshinweise zur Personensicherheit.

Ist die Basisstation mit Spannung versorgt, leuchtet die PWR LED grün und der Balken leuchtet weiß (= die Not-Halt-Ausgänge der Basisstation sind geschlossen).

7.8.2.1 Pinbelegung

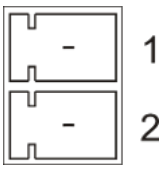


Abb. 7-65: Pinbelegung

KEBA © KEBA 2021

Pin-Nr.	Signalbezeich-nung	Beschreibung
1	-	GND
2	+	24 V DC Spannungsversorgung

7.8.3 Klemmleiste S2

Die Klemmleiste S2 ist direkt verdrahtet und kann für Sicherheitsfunktionen verwendet werden.

Ist die Basisstation mit einem optionalen Schlüsselschalter ausgestattet, liegen an der Klemme S2 die Signale des Bedienelements an. Die Kombination der Pegel zweier Kontakte gibt die Position des Schlüsselschalters an (siehe 7.8.3.1 Pinbelegung).

7.8.3.1 Pinbelegung

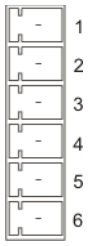
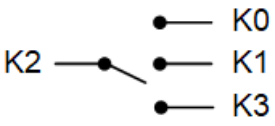


Abb. 7-66: Pinbelegung

Pin-Nr.	Signalbezeich-nung	Beschreibung
1	GND	Erdung
2	n.a.	Keine Verwendung möglich
3	K3	Schlüsselschalterkontakt: Position 3 (rechte Schaltstellung) 
4	K2	Schlüsselschalterkontakt: COMMON
5	K1	Schlüsselschalterkontakt: Position 2 (mittlere Schaltstellung)
6	K0	Schlüsselschalterkontakt: Position 1 (linke Schaltstellung)

7.8.4 Klemmleiste "Signal"

An der Klemme "Signal" kann eine Signalsäule angeschlossen werden.

Die Basisstation wurde von KEBA mit folgenden Signalsäulen getestet:

Hersteller	Produktbezeichnung
PATLITE	LR4-_02LJN

© KEBA 2021

Hersteller	Produktbezeichnung
SPÄLTI	MES-502A-RYGBC(DC24V)

Die Verwendung dieser Signalsäulen wird empfohlen. Weitere Informationen siehe Dokumentation des Herstellers.

Information

Die Klemmleiste "Signal" darf nur zum Anschluss einer Signalsäule für die Anzeige der Betriebs- und Diagnosezustände der Basisstation genutzt werden.

7.8.4.1 Pinbelegung

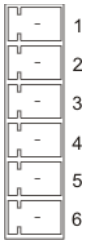


Abb. 7-67: Pinbelegung

Pin-Nr.	Signalbezeichnung	Beschreibung
1	24V	Spannungsversorgung 24 V DC
2	WH	Signalfarbe Transparent/Weiß
3	BU	Signalfarbe Blau
4	Y/O	Signalfarbe Gelb
5	GN	Signalfarbe Grün
6	RD	Signalfarbe Rot

7.8.5 Ethernet

Das Gerät stellt 2 Ethernet-Schnittstellen zur Verfügung. Diese dienen zum Anschluss von Geräten, mit denen das Handbediengerät kommunizieren soll. Die Schnittstellen können über die Kabelausgänge nach außen geführt werden.

7.8.5.1 Pinbelegung

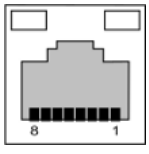


Abb. 7-68: RJ45 Buchse

KEBA © KEBA 2021

Pin-Nr.	Signalbezeichnung		Eingang/Ausgang
1	Tr. Data+	Transmit Data +	Ausgang
2	Tr. Data-	Transmit Data -	Ausgang
3	Re. Data+	Receive Data +	Eingang
4	n.c.	n.c.	---
5	n.c.	n.c.	---
6	Re. Data-	Receive Data -	Eingang
7	n.c.	n.c.	---
8	n.c.	n.c.	---

7.8.6 EtherCAT

Das Gatewaymodul besitzt 2 EtherCAT-Schnittstellen. Die Schnittstellen können über die Kabelausgänge am CB43x oder durch die Öffnung (optional) an der Rückseite des EtherCAT / FSoE-Gateways nach außen geführt werden.

Folgende Steckverbinder können verwendet werden:

Hersteller	Produktbezeichnung
Siemens	6GK1901-1BB10-2AA0 (FastConnect)
Weidmüller	IE-PS-RJ45-FH-BK

Achtung

An den Laschen des Prints muss mit Kabelbindern eine Zugentlastung der angeschlossenen Kabel durchgeführt werden!

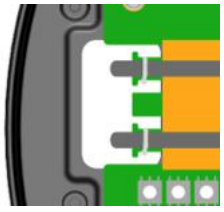


Abb. 7-69: Beispiel: Zwei angeschlossene Kabel mit Kabelbindern als Zugentlastung

© KEBA 2021

7.8.7 Änderungen an der Verkabelung

Information

Informationen zu Änderungen an der Verkabelung:

- Beim Abstecken von Steckverbindungen ist darauf zu achten, dass der Stecker durch Ziehen mit den Fingern an seinen Adern abgesteckt wird (keine spitzen Gegenstände dafür zu Hilfe nehmen).
- Beim Abstecken der RJ45-Stecker ist darauf zu achten, dass der Verriegelungshebel dabei betätigt wird:

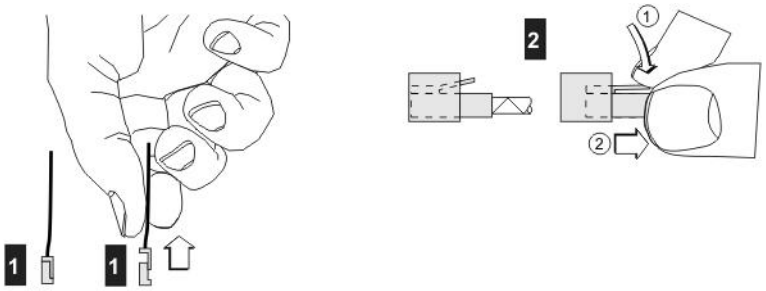


Abb. 7-70: Abstecken des Hauptsteckers und des RJ-45-Steckers

1 ... Hauptstecker	2 ... RJ45-Stecker

7.8.8 Schließen der Basisstation

Um die Basisstation zu schließen, wird das Gehäuse von der Rückwand abgenommen und umgedreht. Danach kann das Gehäuse an der Rückwand aufgelegt und mittels 6 PT30x10-Schrauben (benötigtes Werkzeug - Torx Größe 10), wie in der Abbildung gezeigt, verschraubt werden. Die Schrauben sind im Lieferumfang enthalten.

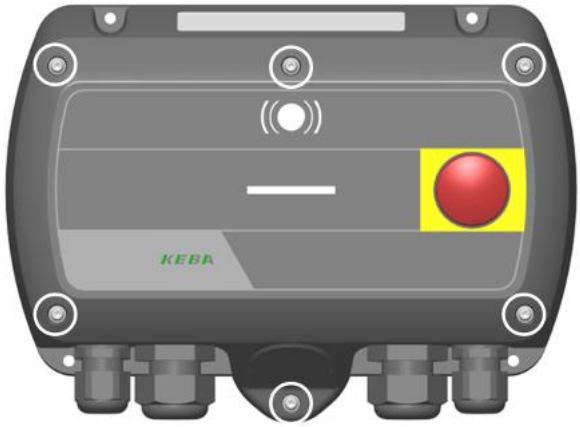


Abb. 7-71: Schrauben für den Zusammenbau

KEBA © KEBA 2021

Information

Informationen zum Schließen der Basisstation:

- Die Dichtung muss sauber und unbeschädigt sein und sich an der richtigen Position befinden.
- Es dürfen keine Kabel eingeklemmt werden.
- Die Basisstation muss mit allen PT30x10-Schrauben wieder verschraubt werden (Drehmoment: 0,85 Nm - 1,15 Nm). Nur dadurch kann die entsprechende Schutzart gewährleistet werden.

Die Basisstation ist betriebsbereit.

7.8.9 Not-Halt

Die Basisstation ist mit einem Not-Halt ausgestattet.

WARNUNG!

Nicht funktionstüchtige Not-Halt-Einrichtungen können fatale Folgen haben! Rot-gelb gekennzeichnete Not-Halt müssen jederzeit und in allen Betriebsarten einer Maschine oder Anlage wirksam sein.

WARNUNG!

Der Not-Halt am nicht verbundenen Handbediengerät ist kein Ersatz für den Not-Halt auf der Maschine. Es muss immer ein stationär fest verdrahteter Not-Halt an der Maschine verfügbar sein.

7.9 Fehlerquittierung

WARNUNG!

Lebensgefahr durch unerwartetes Anfahren der Maschine

Bei einer automatischen Wiedereingliederung, z.B. nach einem Busfehler, wird die CB4xx wieder in den vorherigen Zustand versetzt. Ohne übergeordnete, sichere Maßnahme kann die Maschine wieder anfahren und zu schweren Verletzungen oder Tod führen.

- Sicherstellen, dass die verwendete Sicherheitssteuerung keine automatische Wiedereingliederung des F-Devices vornimmt.

Alle Fehler, die lokal im Wirelesssystem auftreten, müssen an der CB4xx oder am Handbediengerät quittiert werden. Diese Fehler werden an der CB4xx mit einem rot/gelben LED Balken signalisiert.

© KEBA 2021

Eine Quittierung erfolgt durch das Drücken/Entriegeln des Nothalts. Die erfolgte Quittierung wird an der CB4xx durch einen gelb blinkenden LED-Balken signalisiert. Erst danach ist eine softwareseitige Quittierung am F-Host durch das Setzen einer Anwenderquittierung möglich.

KEBA © KEBA 2021

8 Konfiguration

8.1 Box-ID Konfiguration

Die Basisstation besitzt 2 Adressschalter zum Einstellen der Box-ID.

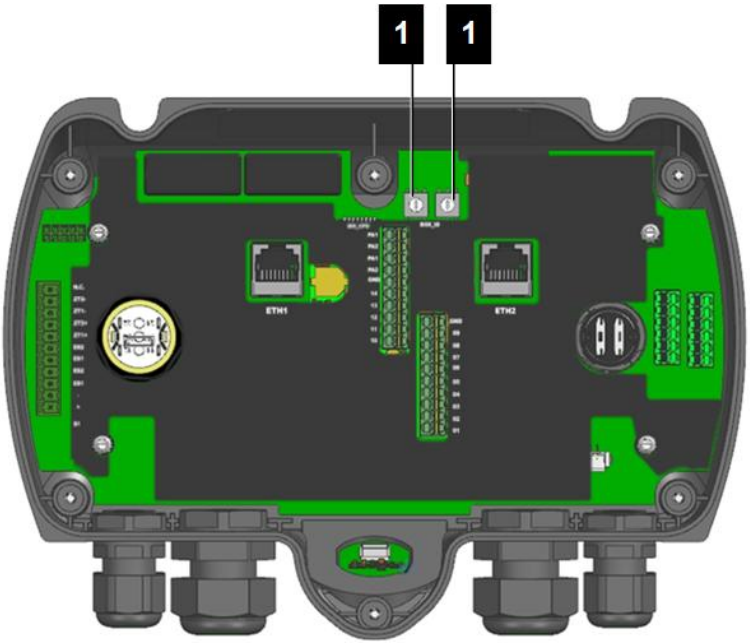


Abb. 8-72: Position der Elemente zur Konfiguration

1 ... Adressschalter	

Die Konfiguration der Box-ID dient zur Identifikation des Geräts. Es kann eine ID von 0 - 255 vergeben werden, welche in der Applikation verwendet werden kann. Dazu dienen zwei Adressschalter, über die die Adresse in Hexadezimal eingestellt werden kann:

Abb. 8-73: Adressschalter

Standardmäßig ist die Box-ID 00 eingestellt.

Beispiele:

Linker Adressschalter	Rechter Adressschalter	Adresse
0	0	0
0	1	1

© KEBA 2021

Linker Adress-schalter	Rechter Adress-schalter	Adresse
0	2	2
...	...	...
0	A	10
...	...	...
1	0	16
1	1	17
...	...	..

Bei einem Verbindungsaufbau mit dem Handbediengerät (Pairing/Remote Pairing) wird die aktuelle Box-ID übermittelt.

Eine Auswertung kann über die Verbindungsprotokolle oder über die Schnittstelle "HWApi" erfolgen.

8.2 F-Adressierung (nur bei CB42x und CB43x)

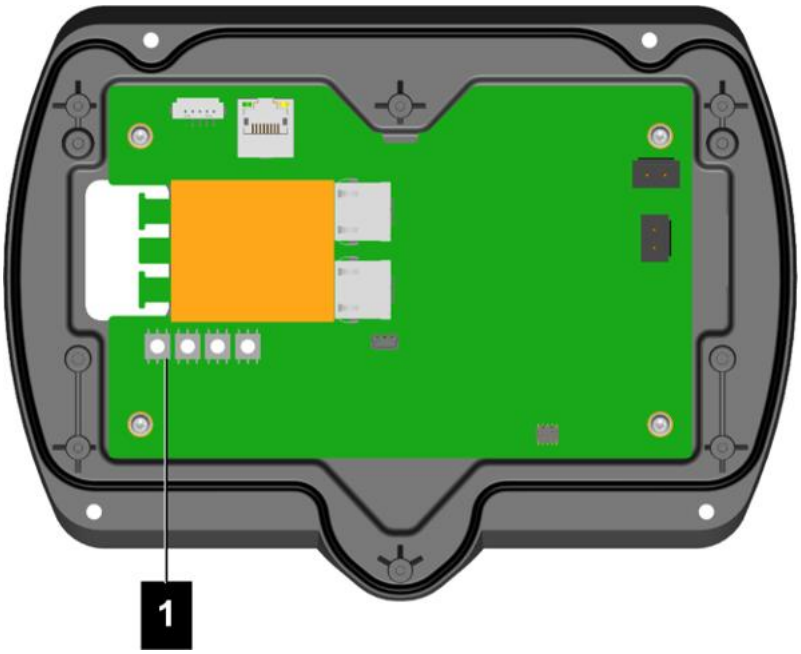
Das Gatewaymodul besitzt 4 Adressschalter zum Einstellen der F-Adressen der jeweiligen Busteilnehmer. Das Einstellen der F-Adressen erfolgt in Hexadezimal.

Im Auslieferzustand ist die F-Adressierung standardmäßig 0.

Information

Die F-Adresse 0000 ist nicht zulässig. Eine ungültige F-Adresse kann zu einem Feldbus-Fehler führen und wird über den Status-LED-Balken der Basisstation signalisiert.

KEBA © KEBA 2021



1 ... Adressschalter	

Zum Ändern der F-Adresse eines Busteilnehmers gehen Sie wie folgt vor:

1) Alle Adressschalter auf „0“ stellen. (Auslieferzustand: alle Adressschalter sind auf 0)
2) Basisstation neustarten und 10 Sekunden warten.
3) Basisstation stromlos setzen.
4) Gewünschte F-Adresse über die Adressschalter eingeben.

Beim nächsten Einschalten der Basisstation blinkt der LED-Status-Balken rot. Nach einem wiederholten Neustart ist die neue F-Adresse gültig.

Für ein Beispiel über die Adressvergabe mit Adressschaltern siehe 8.1 Box-ID Konfiguration.

8.3 Bedienbereichs-Konfiguration (sicherheitsrelevant)

Über den DIP-Switch auf der Basisstation kann der Bedienbereich der Basisstation mit dem Handbediengerät eingestellt werden. Der Bedienbereich muss bei der Inbetriebnahme der Basisstation eingestellt werden. Wenn kein Bedienbereich definiert ist, blinkt der Status-LED-Balken an der Basisstation weiß.

Bedienbereich	Bit 0	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7
Ohne	ON	OFF	OFF	OFF	x	x	x	x
Initialzustand (Sicherer Zustand)	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF
5 m	OFF	ON	OFF	OFF	x	x	x	x
10 m	OFF	OFF	ON	OFF	x	x	x	x

© KEBA 2021

Bedienbereich	Bit 0	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7
15 m	OFF	OFF	OFF	ON	x	x	x	x
20 m	OFF	ON	OFF	ON	x	x	x	x

x ... Position / Stellung des jeweiligen Schalters ist nicht relevant

ON/OFF-Stellung der Schalter

Folgende Darstellung zeigt die Position des DIP-Switches in der geöffneten Basisstation und die Konfiguration des Bedienbereichs.

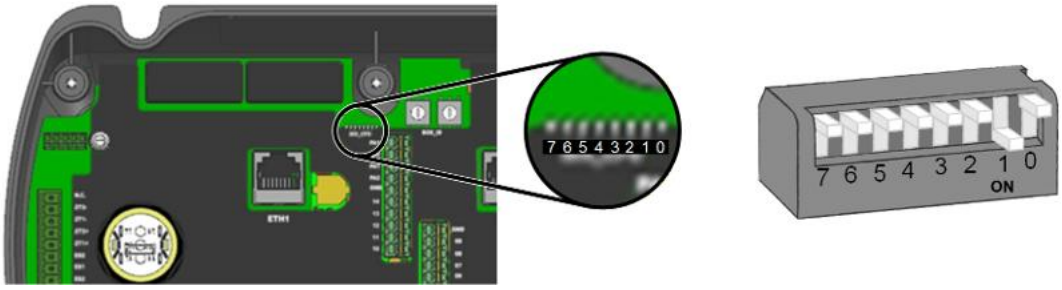


Abb. 8-74: Beispiel: Position des DIP-Switches und eingestellter Bedienbereich von 5 m

Zum Einstellen des Bedienbereichs muss die Basisstation stromlos sein. Gehen Sie wie folgt vor:

1) Alle DIP-Switches auf OFF stellen
2) Basisstation mit Spannung versorgen und ca. 10 sec warten
3) Basisstation stromlos setzen
4) DIP-Switches auf den gewünschten Bedienbereich einstellen

Beim nächsten Einschalten der Basisstation wird die Konfiguration übernommen.

8.4 Gerätekonfiguration (Device Config)

In der Gerätekonfiguration am Handbediengerät können folgende Grundeinstellungen durchgeführt werden:

- Basisstation-Einstellungen
- Erzeugen von Diagnosedaten
- Einstellen der Display-Helligkeit des Handbediengeräts
- Anzeige der Lizenzinformationen
- Netzwerkeinstellungen
- Auslösen eines Neustarts des Handbediengeräts
- Herunterfahren des Handbediengeräts
- Anzeige der Softwareversionen

KEBA © KEBA 2021

Information

Um alle Konfigurationsmöglichkeiten nutzen zu können, muss das Handbediengerät mit der Basisstation vor dem Start der Gerätekonfiguration verbunden werden.

Die Gerätekonfiguration kann vom Desktop aus mittels Doppelklicken auf das Icon **DeviceConfig** gestartet werden.

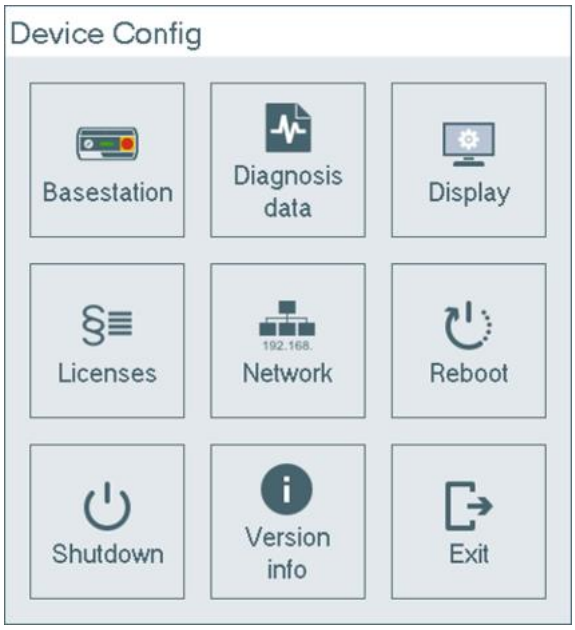


Abb. 8-75: Gerätekonfiguration Hauptmenü

Über **Exit** wird die Gerätekonfiguration wieder verlassen.

8.4.1 Basestation

Durch Drücken von **Basestation** wird das Basisstation-Fenster aufgerufen. In diesem Fenster können Einstellungen für die Basisstation durchgeführt werden.

Information

Das Handbediengerät muss dazu mit der Basisstation verbunden sein.

© KEBA 2021

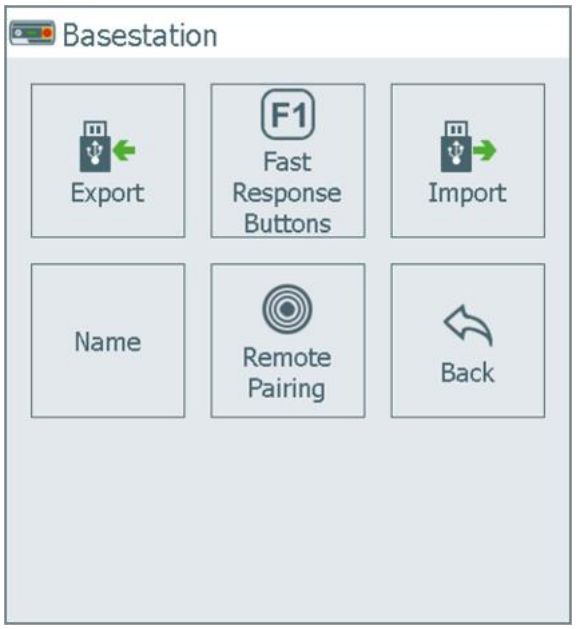


Abb. 8-76: Basestation-Fenster

Bezeichnung	Bedeutung
Export	Export der Einstellungen der verbundenen Basisstation in eine Datei. Informationen, die in der Datei abgelegt werden sollen, können ausgewählt werden. Als Speicherort kann nur ein Massenspeicher am USB (z.B. USB-Stick) verwendet werden. Ist keine Basisstation verbunden, kann diese Funktion nicht ausgewählt werden.
Fast Response Buttons	Konfiguration der Tasten, die direkt auf Ausgänge der Basisstation ausgegeben werden (optional).
Import	Import der Einstellungen für die verbundenen Basisstation aus einer Datei. In der Datei abgelegte Informationen können zum Import ausgewählt werden. Als Quelle kann nur ein Massenspeicher am USB (z.B. USB-Stick) verwendet werden. Ist keine Basisstation verbunden, kann diese Funktion nicht ausgewählt werden.
Name	Namensvergabe der Basisstation (nur Buchstaben und Ziffern verwenden, keine Sonderzeichen verwenden)
Remote Pairing	Konfiguration der Basisstation für Remote Pairing.

Durch Drücken von **Back** kann wieder zum Hauptmenü navigiert werden.

Fast Response Buttons

Durch Drücken von **Fast Response Buttons** wird in das Menü der Fast Response Buttons gewechselt.

Mit den Fast Response Buttons können die Bedienelemente des Handbediengeräts mit den Ausgängen der Basisstation verknüpft werden.

KEBA © KEBA 2021

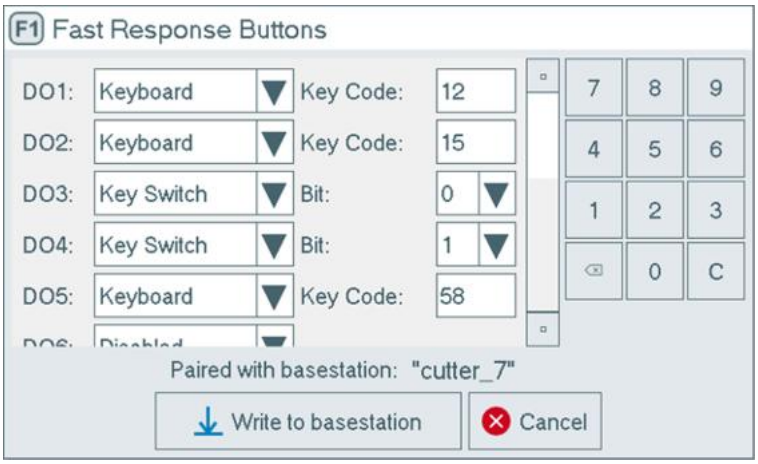


Abb. 8-77: Fast Response Buttons-Fenster

Folgende Möglichkeiten für Fast Response Buttons können in der Dropdown-Liste ausgewählt werden.

Auswahl	Beschreibung
Auto-Detect	Nach der Auswahl muss entweder eine Taste gedrückt werden oder ein Einbauelement betätigt werden, z.B. der Joystick in eine Richtung bewegt werden. Das Ergebnis dieser Aktion wird übernommen.
Keyboard	Es wird der Scancode der Taste verwendet.
Key Switch	Die Anzahl der zur Verfügung stehenden Bits ist von der verwendeten Hardware abhängig.
Joystick	Je Achse werden 2 Bits verwendet.
Push Button	1 Bit
Push Switch	1 Bit
Rotary Switch	Die Anzahl der zur Verfügung stehenden Bits ist von der verwendeten Hardware abhängig.
Select Switch	Die Anzahl der zur Verfügung stehenden Bits ist von der verwendeten Hardware abhängig.
Disabled	Der Ausgang wird nicht verwendet.

Mit **Write to basestation** werden die Einstellungen auf die Basisstation übertragen und auf das vorhergehende Fenster zurück gewechselt. Mit **Cancel** wird das Fenster verlassen, ohne die geänderten Einstellungen zu speichern.

Name

Durch Drücken von **Name** wird in das Menü der Namensvergabe der Basisstation gewechselt.

© KEBA 2021

Abb. 8-78: Namensvergabe der Basisstation

Bezeichnung	Bedeutung
Name:	Namensvergabe der Basisstation (keine Sonderzeichen erlaubt)

Mit **Write to basestation** werden die Einstellungen auf der Basisstation übertragen und auf das vorhergehende Fenster zurück gewechselt. Mit **Cancel** wird das Fenster verlassen ohne, die geänderten Einstellungen zu speichern.

Remote Pairing

Durch Drücken von **Remote Pairing** wird in das Menü der Grundeinstellungen des Remote Pairing gewechselt.

In diesem Dialog können die Grundeinstellungen zur Verwendung von Remote Pairing durchgeführt werden.

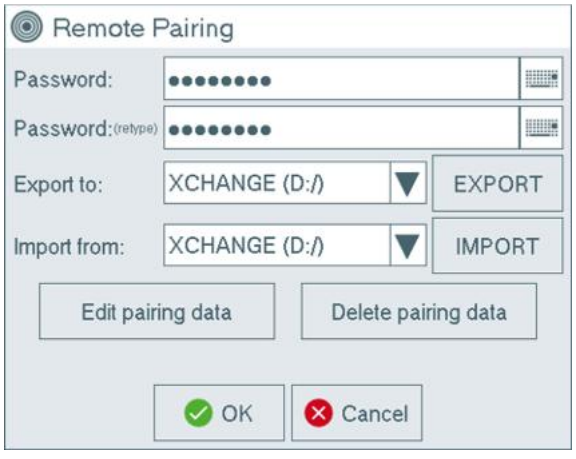


Abb. 8-79: Grundeinstellungen des Remote Pairing

Bezeichnung	Bedeutung
Passwort	Vergabe eines Passwortes zur späteren Nutzung von Remote Pairing. Dient zum Schutz vor Missbrauch.

KEBA © KEBA 2021

Bezeichnung	Bedeutung
Export to	Exportieren der Liste mit den Basisstationen, mit denen das Handbediengerät bereits verbunden war. (Bei jedem "Pairing"-Vorgang wird die Kennung (MAC-Adresse und Name) der Basisstation am verbundenen Handbediengerät hinterlegt.) Diese Liste kann bei der Funktionalität von "Remote Pairing" zur Auswahl der Basisstation verwendet werden.
Import from	Importieren der Liste der Basisstationen am Handbediengerät, um bei Remote Pairing eine Auswahl der Basisstation über den Namen zu ermöglichen.
Edit pairing data	Bearbeiten der Liste der Basisstationen
Delete pairing data	Löschen der Liste der Basisstationen

Mit **OK** werden die Einstellungen gespeichert und auf das vorhergehende Fenster zurück gewechselt. Mit **Cancel** wird das Fenster verlassen, ohne die geänderten Einstellungen zu speichern.

Information

*Importierte und geänderte Verbindungsdaten und auch das Löschen der Verbindungsdaten kann durch Drücken von **Cancel** nicht rückgängig gemacht werden.*

Edit pairing data

Durch Drücken von **Edit pairing data** wird in die Liste der Daten des Remote Pairing gewechselt.

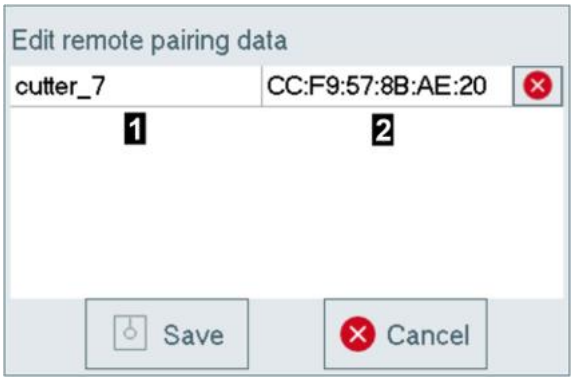


Abb. 8-80: Liste der Daten des Remote Pairing

1 ... Name der Basisstation	2 ... MAC-Adresse der Basisstation

Durch Drücken des roten **X** direkt neben einer Verbindung kann diese aus der Liste gelöscht werden.

Mit **Save** werden die Einstellungen gespeichert und auf das vorhergehende Fenster zurück gewechselt. Mit **Cancel** wird das Fenster verlassen, ohne die geänderten Einstellungen zu speichern.

© KEBA 2021

8.4.2 Diagnosis data

Durch Drücken von **Diagnosis Data** können Diagnose Daten des Handbediengeräts auf einen USB-Stick gespeichert werden.

Gehen Sie dazu wie folgt vor:

1) Anstecken eines USB-Sticks am Handbediengerät.
2) Drücken von **Diagnosis Data**.
3) Im Dialog USB-Stick auswählen.

Die Diagnose Daten werden auf den USB-Stick kopiert.

Information

Der USB-Stick darf nie während eines Speichervorgangs abgezogen werden! Sonst kann es zu Datenverlust kommen.

8.4.3 Display

Durch Drücken von "Display" wird das Display-Fenster aufgerufen.

Durch Drücken von "Back" kann wieder zum Hauptmenü navigiert werden.

Brightness

Durch Drücken von "Brightness" wird die Maske für die Helligkeitseinstellung angezeigt. Über den Schieberegler wird die Helligkeit des Displays eingestellt.

Abb. 8-81: Helligkeitseinstellungen

Mit "OK" werden die Einstellungen gespeichert und auf die vorhergehende Maske zurück gewechselt. Mit "Cancel" wird das Fenster verlassen, ohne die geänderten Einstellungen zu speichern.

KEBA © KEBA 2021

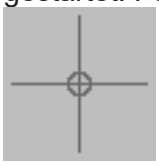
Information

Wenn die Helligkeit des Displays auf mehr als 70 % eingestellt wird, wird die Leistung von CPU und GPU vermindert, um eine Erhöhung der Temperatur im Inneren des Geräts zu verhindern.

Information

Führen Sie die Kalibrierung mit einem Touchstift durch.

Durch Drücken von **Touch Calibration** wird die Touchscreen Kalibrierung gestartet. Folgendes Symbol wird für die Kalibrierung verwendet:



Für die Kalibrierung wird das Symbol mehrmals der Reihe nach in allen 4 Ecken des Displays angezeigt. Die Reihenfolge der Anzeige ist links oben, rechts oben, links unten und rechts unten. Bei jeder Anzeige muss die Mitte des Symbols so präzise wie möglich berührt werden. Dabei soll darauf geachtet werden, die Punkte nur kurz auszuwählen - zu langes Drücken führt zu falscher Kalibrierung.

Nach erfolgreicher Kalibrierung wird das Kalibrierungsfenster geschlossen und die Kalibrierung des Touchscreens ist abgeschlossen.

8.4.4 Licenses

Durch Drücken von **Licenses** werden die Lizenzinformationen angezeigt.

Mit **OK** wird das Fenster verlassen.

8.4.5 Network

Durch Drücken von "Network" wird das Netzwerk-Fenster aufgerufen. In diesem Fenster können die Netzwerkeinstellungen für verfügbare Ethernetschnittstellen geändert werden.

© KEBA 2021

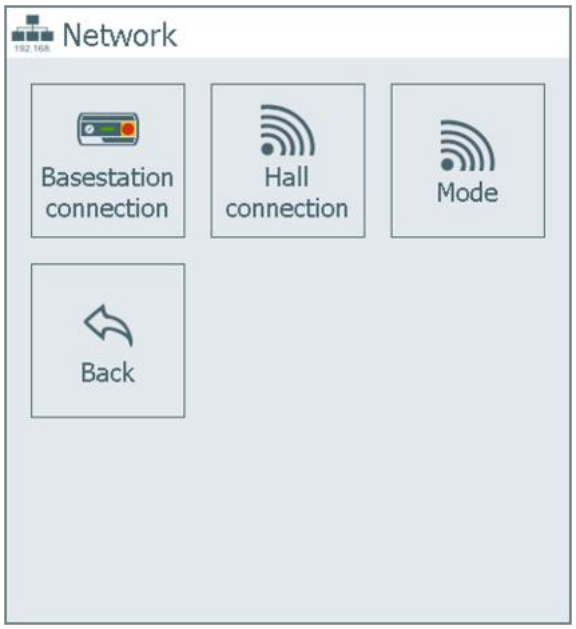


Abb. 8-82: Netzwerk-Fenster

Bezeichnung	Bedeutung
Basestation connection	Netzwerkeinstellungen der Basisstation
Hall connection	Netzwerkeinstellungen für das Hallennetzwerk
Mode	Verhalten zwischen Handbediengerät und Basisstation

Durch Drücken von "Back" kann wieder zum Hauptmenü navigiert werden.

Basestation connection

Durch Drücken von "Basestation connection" wird in das Menü der Basisstation gewechselt.

KEBA © KEBA 2021

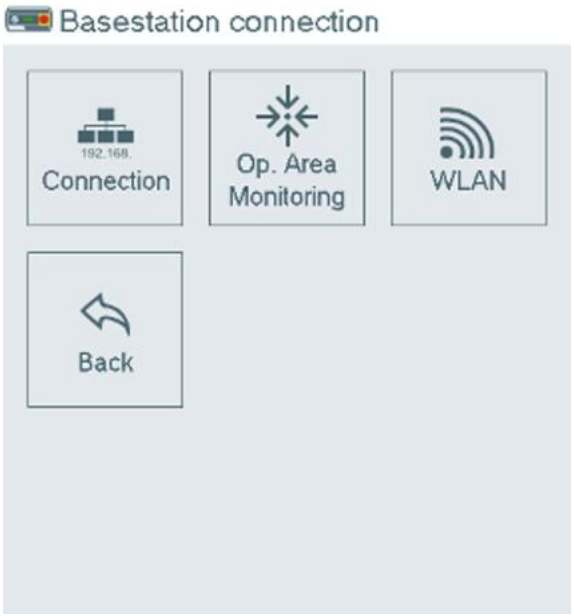


Abb. 8-83: Basisstation-Fenster

Bezeichnung	Bedeutung
Connection	Konfiguration der Netzwerkeinstellungen der Basisstation.
Op. Area Monitoring	Konfiguration des Kommunikationskanals der Bedienbereichs-überwachung.
WLAN	Konfiguration des generierten WLANs zwischen Basisstation und Handbediengerät.

Durch Drücken von "Back" kann wieder zum Netzwerk-Fenster navigiert werden.

Connection

Durch Drücken von "Connection" wird in das Konfigurationsfenster der Netzwerkeinstellungen der Basisstation gewechselt.

Die Netzwerkadresse kann entweder automatisch über DHCP bezogen oder manuell konfiguiert werden.

© KEBA 2021

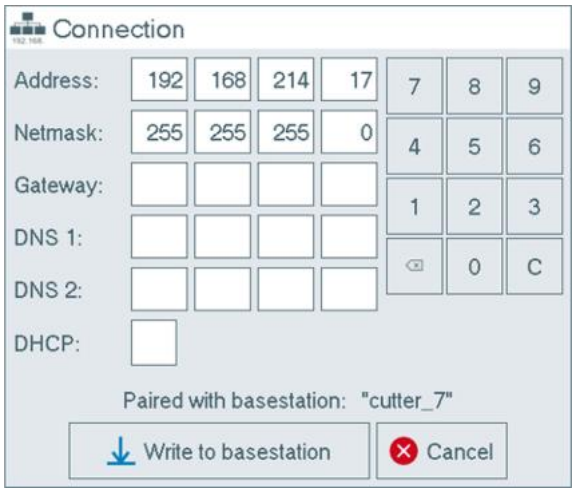


Abb. 8-84: Konfiguration der Netzwerkeinstellungen

Bezeichnung	Bedeutung
Address:	IP-Adresse des Handbediengeräts
Netmask:	Zugehörige Subnetz-Maske
Gateway:	Standard-Gateway
DNS 1:	DNS Server (1)
DNS 2:	DNS Server (2)
DHCP:	Durch Aktivieren von "DHCP" wird die IP-Adresse automatisch über einen DHCP-Server bezogen und die restlichen Eingabe-zeilen deaktiviert.

Mit "Write to basestation" werden die Einstellungen auf die Basisstation übertragen und auf das vorhergehende Fenster zurück gewechselt. Mit "Cancel" wird das Fenster verlassen, ohne die geänderten Einstellungen zu speichern.

Op. Area Monitoring

Durch Drücken von "Op. Area Monitoring" wird in das Konfigurationsfenster des Kommunikationskanals der Bedienbereichsüberwachung gewechselt.

Für die Bedienbereichsüberwachung können der Kanal und das Funkband ausgewählt werden.

Information

Um Störungen zu vermeiden, darf der ausgewählte Kanal für die Bedienbereichsüberwachung nicht mit dem Kanal des WLAN übereinstimmen. Es darf jedoch ausschließlich der Kanal und nicht das Funkband verändert werden.

Wenn mehrere Geräte mit Bedienbereichsüberwachung parallel betrieben werden, müssen ebenso unterschiedliche Kommunikationskanäle genutzt werden. Auf einer Fläche von 500m² sollten nicht mehr als fünf aktive Verbindungen parallel betrieben werden.

KEBA © KEBA 2021

Abb. 8-85: Konfiguration der Bedienbereichsüberwachung

Bezeichnung	Bedeutung
Band:	Frequenz für die Bedienbereichsüberwachung
Channel:	Kanal für die Bedienbereichsüberwachung

Mit "Write to basestation" werden die Einstellungen auf der Basisstation übertragen und auf das vorhergehende Fenster zurück gewechselt. Mit "Cancel" wird das Fenster verlassen, ohne die geänderten Einstellungen zu speichern.

WLAN

Durch Drücken von "WLAN" wird in das Konfigurationsfenster des generierten WLANs zwischen Basisstation und Handbediengerät gewechselt.

Für dieses WLAN können der Kanal und das Funkband ausgewählt werden, alle anderen WLAN-Parameter werden von der Basisstation selbstständig festgelegt und dem Handbediengerät mitgeteilt.

Information

Wenn die Bedienbereichsüberwachung genutzt wird, sollte die WLAN-Kommunikation zur Basisstation auf dem Frequenzband 5 GHz betrieben werden.

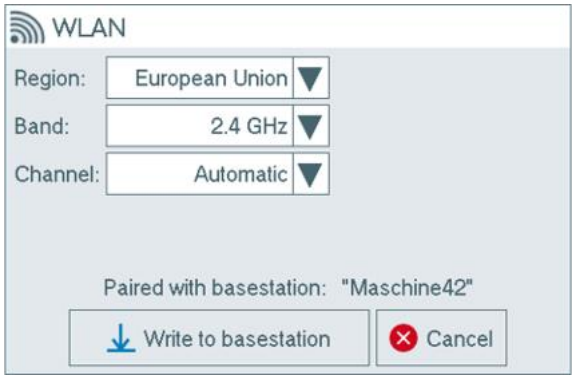


Abb. 8-86: WLAN-Einstellungen

© KEBA 2021

Bezeichnung	Bedeutung
Region:	Region in der die Basisstation betrieben wird
Band:	WLAN-Frequenz
Channel:	WLAN-Kanal

Mit "Write to basestation" werden die Einstellungen auf die Basisstation übertragen und auf das vorhergehende Fenster zurück gewechselt. Mit "Cancel" wird das Fenster verlassen, ohne die geänderten Einstellungen zu speichern.

Hall connection

Durch Drücken von "Hall connection" wird in das Konfigurationsfenster des Hallennetzwerks gewechselt.

Die Netzwerkadresse kann auf folgende Weisen konfiguriert werden:

- DHCP: Hiermit ist die automatische Einbindung in ein bestehendes Netzwerk ohne manuelle Konfiguration möglich.
- Manuell: Die einzelnen vier Segmente der Netzwerkadressen müssen dabei über das numerische Eingabepanel eingegeben werden (entsprechende Segmente anwählen).

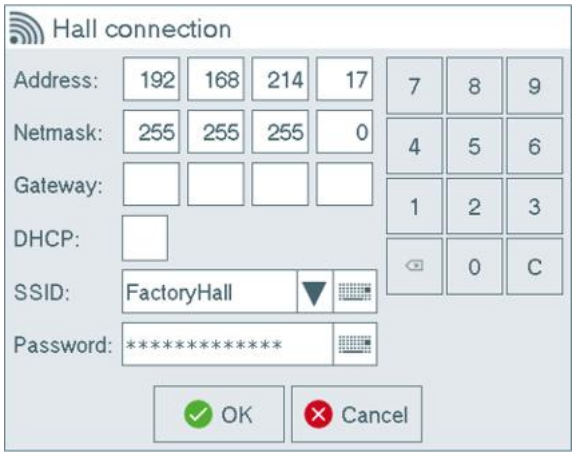


Abb. 8-87: Konfiguration des Hallennetzwerks

Bezeichnung	Bedeutung
Adress:	IP-Adresse des Handbediengeräts
Netmask:	Zugehörige Subnetz-Maske
Gateway:	Standard-Gateway
DHCP:	Durch Aktivieren von "DHCP" wird die IP-Adresse automatisch über einen DHCP-Server bezogen und die restlichen Eingabezeilen deaktiviert.
SSID:	SSID des WLANs (aus der Liste der empfangenen WLANs kann eines gewählt werden)
Password	Passwort des WLANs

KEBA © KEBA 2021

Mode

Durch Drücken von "Mode" wird in das Menü der Parameter gewechselt.

Achtung

Bei der Verwendung des Hallennetzwerkes ist sicherzustellen, dass die Einstellungen des WLANs (z.B. Router, Zugangspunkt, ...) einen ausreichend sicherer Betrieb gewährleisten - siehe dazu 1.3 bestimmungsgemäßer Gebrauch.

Mit diesen Parametern kann das Verhalten des Handbediengeräts mit der Basisstation festgelegt werden.

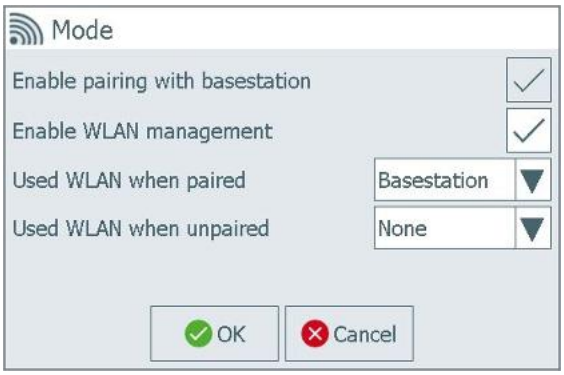


Abb. 8-88: Parametereinstellungen

Bezeichnung	Bedeutung
Enable pairing with basestation	Pairing (Aufbau einer sicheren Verbindung) zwischen Handbediengerät und Basisstation erlauben
Enable WLAN management	Aktivierung der WLAN Erkennung. Ohne Auswahl ist keine Verbindung zu einem WLAN möglich.
Used WLAN when paired	Auswahl des WLANs, mit dem sich das Handbediengerät im gekoppelten Zustand verbindet: ● Basestation: Basisstation ● Hall: Hallennetzwerk ● None: keines
Used WLAN when unpaired	Auswahl des WLANs, mit dem sich das Handbediengerät verbindet, sobald die sichere Verbindung zur Basisstation getrennt wird. ● Hall: Hallennetzwerk ● None: keines

Mit "OK" werden die Einstellungen gespeichert und auf das vorhergehende Fenster zurück gewechselt. Mit "Cancel" wird das Fenster verlassen, ohne die geänderten Einstellungen zu speichern.

© KEBA 2021

8.4.6 Reboot

Durch Drücken von **Reboot** wird ein Neustart des Handbediengeräts ausgelöst.

8.4.7 Shutdown

Durch Drücken von **Shutdown** wird das Handbediengerät heruntergefahren.

8.4.8 Version info

Durch Drücken von "Version info" werden Versionsinformationen über installierte Softwarekomponenten angezeigt:

- Windows Basisimage
- BIOS
- Basestation Bootloader (bei Verbindung mit einer Basisstation)
- Basestation Firmware (bei Verbindung mit einer Basisstation)
- Baseboard OpControl Bootloader
- Baseboard OpControl Firmware

Abb. 8-89: Versionsinformation

Mit **OK** wird das Fenster verlassen.

Information

Die Anzahl der aufgelisteten Versionsinformationen können je nach Ausstattung des Handbediengeräts bzw. der Basisstation abweichen.

KEBA © KEBA 2021

8.5 PROFINET-Konfiguration (nur bei CB42x)

Information

Vor der Konfiguration muss die GSDML Datei der CB420 in das verwendete Projektierungstool geladen werden. Die Datei kann vom KEBA Dataportal heruntergeladen werden.

Folgende Eingaben müssen bei der PROFINET-Konfiguration für das Gatewaymodul vorgenommen werden:

Safetyparameter

Parameter	Beschreibung
F_SIL	SIL1; SIL2; SIL3
F_Source_Add	Angabe der F-Adresse des Host (dec)
F_Dest_Add	Angabe der F-Adresse der CB42x (dec)
F_WD_Time	Watchdogzeit der CB42x Der Wert kann zwischen 50 ms und 2000 ms eingestellt werden. Es wird empfohlen die Watchdogzeit nicht unter 100 ms einzustellen.

Das Gatewaymodul unterstützt keine iParameter. iParameter können daher weder im verwendeten Projektierungstool noch auf andere Weise gesetzt werden.

PROFINET RT Config

Der Parameter "Update Time" für die PROFINET Cycle Time darf nicht unter 4 ms gewählt werden.

8.5.1 Prozessdatenabbild

Slot 1: System Status

Eingangsdaten

Bit	Name	Typ	Adresse	Beschreibung
Bit 0	Verbunden	BOOL	%I X.0	0 = keine sichere Verbindung zwischen Handbediengerät und Basisstation 1 = Handbediengerät und Basisstation verbunden
Bit 1-7			%I X.1 - 7	reserviert

Ausgangsdaten

Keine.

© KEBA 2021

Slot 2: Safety PDU PROFIsafe

Eingangsdaten

Bit	Name	Typ	Adresse	Beschreibung
Bit 0	Zustimmtaster	BOOL	%I X.0	1 = Stellung „Zustimmung“
Bit 1	Zustimmtaster Panik	BOOL	%I X.1	0 = Stellung „Panik“
Bit 2	Not-Halt	BOOL	%I X.2	1 = Stellung „entriegelt“
Bit 3	Pairing	BOOL	%I X.3	1 = KeTop ist in Betriebsart „Standard Pairing“ verbunden
Bit 4	Remote Pairing	BOOL	%I X.4	1 = KeTop ist in Betriebsart „Remote Pairing“ verbunden
Bit 5	WAL3	BOOL	%I X.5	1 = KeTop befindet sich in WAL Zone 3 (Übertretungsbereich)
Bit 6	WAL2	BOOL	%I X.6	1 = KeTop befindet sich in WAL Zone 2 (Toleranzbereich)
Bit 7	WAL1	BOOL	%I X.7	1 = KeTop befindet sich in WAL Zone 1 (Bedienbereich)

Prozessdaten Zustimmtaster

Systemzustand	Wert Bit 0	Wert Bit 1
Zustimmtaster "nicht betätigt"	0	1
Zustimmtaster "betätigt"	1	1
Zustimmtaster "Panik"	0	0

Prozessdaten Hot-Halt

Systemzustand	Wert Bit 2
Not-Halt "betätigt"	0
Not-Halt "entriegelt"	1

Prozessdaten Verbindungsbetriebsart

Systemzustand	Wert Bit 3	Wert Bit 4
Kein Handterminal verbunden	0	0
Handterminal "Standard Pairing"	1	0
Handterminal "Remote Pairing"	0	1

Prozessdaten Wirkbereich

Systemzustand	Wert Bit 5	Wert Bit 6	Wert Bit 7
Kein Wirkbereich parametriert/ kein KeTop an der Basisstation verbunden	0	0	0
Handterminal im Arbeitsbereich	0	0	1
Handterminal im Warnbereich	0	1	0
Handterminal im Übertretungsbereich	1	0	0

KEBA © KEBA 2021

Ausgangsdaten
Keine.

> ***Information***
>
> *Im nichtverbundenen Zustand befindet sich Bit 1 im Zustand 0 (= Stellung "Panik"). Bit 1 nur mit einem verbundenen Handbediengerät auswerten.*
>
> *Im sicheren Zustand ist das gesamte Prozessdatenabbild = "0".*

Slot 3: Keypad

Ein Bit entspricht einer betätigten Taste. Das Tastaturmapping ist im Variantendatenblatt des Gerätes zu finden.

Eingangsdaten

Byte	Name	Typ	Adresse	Beschreibung
1-4	Tastatur	DWORD	%IDW X	Tastaturmapping lt. Variantendatenblatt

Ausgangsdaten

Byte	Name	Adresse	Beschreibung
1	LED	%QB X	LED 1-8 ON/OFF
2	LED blink	%QB X+1	LED 1-8 blinken

Slot 4: Operator Control Elements

Eingangsdaten

Byte	Name	Typ	Adresse	Beschreibung
1	Schaltelement 1	Byte	%IB X	Zustand Schaltelement 1
2	Schaltelement 2	Byte	%IB X+1	Zustand Schaltelement 2

Ausgangsdaten

Byte	Name	Adresse	Beschreibung
1	LED	%QB X	LED 1-2 ON/OFF
2	LED blink	%QB X+1	LED 1-2 blinken

Slot 5: Handwheel

Eingangsdaten Byte 0-1

Byte	Name	Typ	Adresse	Beschreibung
Byte 0-1	Handwheelcounter	WORD	%IW X+1	Handwheelcounter

© KEBA 2021

Eingangsdaten Byte 2

Bit	Name	Typ	Adresse	Beschreibung
Bit 1	Handwheel pushbutton	BOOL	%I X +2.0	Handrad gedrückt
Bit 2-8			%I X	reserviert

Ausgangsdaten
Keine.

8.6 EtherCAT / FSoE-Konfiguration (nur bei CB43x)

Information

Vor der Konfiguration muss die ESI-XML-Datei ins verwendete Projektierungstool geladen werden.

Die ESI-XML-Datei enthält die kompletten Geräte-Eigenschaften eines EtherCAT-Slaves im XML-Format. Sie enthält alle Informationen für den EtherCAT- oder FSoE-Master: Funktionen, Einstellungen und das Prozessdatenabbild.

Folgende Eingaben müssen bei der EtherCAT / FSoE-Konfiguration für das Gatewaymodul vorgenommen werden:

Safetyparameter

Parameter	Beschreibung
F_SIL	SIL1; SIL2; SIL3
F_Source_Add	Angabe der F-Adresse des Host (dec)
F_Dest_Add	Angabe der F-Adresse der CB43x (dec)
F_WD_Time	Watchdogzeit der CB43x Der Wert kann zwischen 50 ms und 2000 ms eingestellt werden. Es wird empfohlen die Watchdogzeit nicht unter 100 ms einzustellen.

FSoE-Taktzeit

Eine FSoE-Taktzeit von 100 ms wird empfohlen.

8.6.1 Prozessdatenabbild

Eingangsdaten Tastatur

Ein Bit entspricht einer betätigten Taste. Das Tastaturmapping ist im Variantendatenblatt des Gerätes zu finden. Die Adressen hängen von der EtherCAT-Konfiguration ab.

KEBA © KEBA 2021

KBI	Name	Typ	Adresse	Beschreibung
0 - 31	Keyboard	BIT	%Qxx.xx	Tastaturzuordnung entsprechend dem Datenblatt

Ausgangsdaten Tastatur (LEDs)

Byte	Name	Typ	Adresse	Beschreibung
1	ON0-7	BYTE	%Qxx.xx	LED 1 - 8 An/Aus
2	BLINK0-7	BYTE	%Qxx.xx	LED 1 - 8 Blinken

Ausgangsdaten Drucktaster

Wert	Name	Typ	Adresse	Beschreibung
ON0-3	LED on	4-BIT	%Qxx.xx	Drucktaster LED 1 - 4 An
BLINK0-3	Operator control 2	4-BIT	%Qxx.xx	Drucktaster LED 1 - 4 Blinken

Modul 1 (FSoE)

Prozessdaten Zustimmtaster

Systemzustand	Wert Bit 0	Wert Bit 1
Zustimmtaster "nicht betätigt"	0	1
Zustimmtaster "betätigt"	1	1
Zustimmtaster "Panik"	0	0

Prozessdaten Hot-Halt

Systemzustand	Wert Bit 2
Not-Halt "betätigt"	0
Not-Halt "entriegelt"	1

Prozessdaten Verbindungsbetriebsart

Systemzustand	Wert Bit 3	Wert Bit 4
Kein Handterminal verbunden	0	0
Handterminal "Standard Pairing"	1	0
Handterminal "Remote Pairing"	0	1

Prozessdaten Wirkbereich

Systemzustand	Wert Bit 5	Wert Bit 6	Wert Bit 7
Kein Wirkbereich parametriert/ kein KeTop an der Basisstation verbunden	0	0	0
Handterminal im Arbeitsbereich	0	0	1
Handterminal im Warnbereich	0	1	0
Handterminal im Übertretungsbereich	1	0	0

© KEBA 2021

Ausgangsdaten
Keine.

> ***Information***
>
> *Im nichtverbundenen Zustand befindet sich Bit 1 im Zustand 0 (= Stellung "Panik"). Bit 1 nur mit einem verbundenen Handbediengerät auswerten.*
>
> *Im sicheren Zustand ist das gesamte Prozessdatenabbild = "0".*

Status "Working Counter"

Wert	Name	Typ	Beschreibung
WcState	Working Counter Status	BIT	0 = gültige Echtzeitkommunikation im letzten Zyklus 1 = ungültige Echtzeitkommunikation

System Status (InfoData)

Wert	Name	Typ	Adresse	Beschreibung
State	EtherCAT Status	UINT		0x____1 = Slave in Status "INIT" 0x____2 = Slave in Status "PREOP" 0x____3 = Slave in Status "BOOT" 0x____4 = Slave in Status "SAFEOP" 0x____8 = Slave in Status "OP" 0x001_ = Slave signalisiert Fehler 0x002_ = Ungültig "vendorId, productCode...read" 0x004_ = Initialisierungsfehler aufgetreten 0x008_ = Slave abgeschaltet

8.7 Ruhezustand konfigurieren

Mittels DIP-Switch im Anschlussschacht des Handbediengeräts (siehe 4.6.1 Anschlussschacht) kann das Hochlaufverhalten aus dem Ruhezustand konfiguriert werden.

Schalterstellung OFF (Standardeinstellung)

Befindet sich der Schalter auf Position "STBY_OFF", ist ein schneller Hochlauf des Handbediengeräts nicht möglich. Im Ruhezustand wird die CPU nicht weiter mit Strom versorgt. Dadurch ist eine länger Akkulaufzeit (ca. 15 Tage) möglich.

KEBA © KEBA 2021

Schalterstellung ON

Befindet sich der Schalter auf Position "STBY_ON", ist ein schneller Hochlauf und Wiederherstellen des letzten Zustandes ("Suspend to RAM") möglich. Im Ruhezustand wird die CPU weiter mit Strom versorgt. Dadurch verkürzt sich die Akkulaufzeit (auf ca. 2 Tage).

8.8 Fernzugriff auf das KeTop

Information

Auf dem Gerät ist die Standardkonfiguration aktiv. Fernzugriffe von außen (wie z.B. die Funktion "Ping") sind deaktiviert.

Die folgende Beschreibung ist nur für Handbediengeräte mit Windows 10 gültig.

Über das Setup "WindowsCustomizingSetup" können verschiedene Fernzugriffsdienste aktiviert werden.

Sicherheitsinformation

Die Aktivierung des Fernzugriffs ist ein IT-Sicherheitsrisiko aufgrund möglicher unerlaubter Zugriffe auf das Gerät.

Folgende Dienste können aktiviert werden:

- Remote Desktop (RDP): Dieser Dienst ermöglicht den Zugriff auf das Gerät über einen Remote Desktop Client.
- Server Message Block File Sharing (SMB): Dieser Dienst ermöglicht den Zugriff auf das Gerät über freigegebene Ordner.
- ICMP (für Ping): Dieser Dienst ermöglicht es, die Ethernet-Verbindung zum Gerät mit "ping" zu überprüfen.
- KeStudio: Dieser Dienst erstellt Regeln für die Firewall, damit KeStudio genutzt werden kann.

Installation

Um einen Dienst zu installieren, gehen Sie wie folgt vor:

1) Aufruf des Setups über "Programme und Funktionen" - "WindowsCustomizingSetup".
2) Klicken auf "Change".
3) Auswählen des gewünschten Dienstes.

Dienst	Setup Name
Remote Desktop	`RDP activation`
Server Message Block File Sharing	`SMB activation`

© KEBA 2021

Dienst	Setup Name
ICMP	`PING activation`
KeStudio	`KeStudio activation`

4) Klicken auf den schwarzen Auswahlpfeil neben dem ausgewählten Dienst.
5) Auswählen von "Entire Feature will be installed on local hard drive".
6) Klicken auf "Next" - "Change" - "Finish", um die Installation abzuschließen.

Deinstallation

Um einen Dienst zu deinstallieren, gehen Sie wie folgt vor:

1) Aufruf des Setups über "Programme und Funktionen" - "WindowsCustomizingSetup".
2) Klicken auf "Next" - "Change".
3) Auswählen des zu deinstallierenden Dienstes.
4) Klicken auf den schwarzen Auswahlpfeil neben dem ausgewählten Dienst.
5) Auswählen von "Entire feature will be unavailable".
6) Klicken auf "Next" - "Change" - "Finish", um die Deinstallation abzuschließen.

8.8.1 Fernzugriff über OpenSSH

OpenSSH ermöglicht einen sicheren Fernzugriff auf das T15xWL über das SSH-Protokoll. Der OpenSSH-Server ist standardmäßig nicht auf dem Gerät installiert und kann über die Windows-Einstellungen nachinstalliert werden.

Installation

Um den OpenSSH-Server zu installieren, gehen Sie wie folgt vor:

1) Windows-Einstellungen über die Tastenkombination Windows-Taste + I oder über das Startmenü öffnen.
2) Zu System navigieren.
3) Optionale Features auswählen.
4) Feature hinzufügen auswählen.
5) Im Suchfeld OpenSSH eingeben.
6) OpenSSH Server aus der Liste auswählen.
7) Installieren (Add) auswählen.

Der OpenSSH-Server ist installiert.

Der Zugriff auf den OpenSSH-Server erfolgt über den TCP-Port 22, sofern keine Einschränkungen durch Firewall-Regeln bestehen.

KEBA © KEBA 2021

Information

Für die Installation des OpenSSH-Servers ist eine aktive Internetverbindung erforderlich. Das Feature wird über die optionalen Windows-Funktionen bezogen.

Deinstallation

Um den OpenSSH-Server zu deinstallieren, gehen Sie wie folgt vor:

1) Windows-Einstellungen über die Tastenkombination Windows-Taste + I oder über das Startmenü öffnen.
2) Zu System ► Optionale Features navigieren.
3) In der Liste der installierten Features nach OpenSSH Server suchen.
4) Entfernen "Remove" auswählen.

Der OpenSSH-Server ist deinstalliert.

8.9 Security-Einstellungen

Folgende Security-Einstellungen stehen zur Verfügung:

- Whitelisting über AppLocker
- Kiosk Desktop
- KEBA Write Filter

Im Auslieferungszustand ist keine Anwendung vorinstalliert.

Whitelisting über AppLocker

Über den Applocker wird das Ausführen von Programmen, die nicht in einer Liste (Whitelist) registriert und mit Ausführungsregeln hinterlegt sind, geblockt.

Kiosk Desktop

Die Anpassung des Betriebssystems bietet die Möglichkeit, den Benutzerzugriff direkt auf das KeTop einzuschränken.

KEBA Write Filter

Durch die Installation dieser Funktion wird das Dateisystem durch den KEBA Write Filter geschützt.

© KEBA 2021

Information

Sobald KeWF aktiv ist, kann kein Setup mehr ausgeführt werden. Der KeWF muss (durch einen Administrator) manuell gestoppt werden, um eine Änderung durch ein Setup durchführen zu können. Das Feature KeWF selbst kann ebenfalls nicht deinstalliert werden, solange der Schreibfilter aktiv ist.

Um KeWF manuell zu stoppen, eine Kommandozeile öffnen und folgenden Befehl ausführen:

```
net stop KeWF <enter>
```

8.9.1 (De-) Installation

Im Auslieferzustand sind keine Komponenten des Security Setups vorinstalliert.

Installation

Um einen Dienst zu installieren, gehen Sie wie folgt vor:

1) Aufruf des Setups über "Programme und Funktionen" - "WindowsSecuritySetup".
2) Klicken auf "Change".
3) Auswahl des gewünschten Dienstes.
4) Klicken auf Auswahlpfeil neben dem gewählten Dienst - "Entire Feature will be installed on local hard drive".
5) Klicken auf "Next" - "Change" - "Finish", um die Installation abzuschließen.

Der jeweilige Dienst ist installiert und wird nach einem Neustart aktiv.

Deinstallation

Um einen Dienst zu deinstallieren, gehen Sie wie folgt vor:

1) Aufruf des Setups über "Programme und Funktionen" - "WindowsSecuritySetup".
2) Klicken auf "Change".
3) Auswahl des gewünschten Dienstes.
4) Klicken auf Auswahlpfeil neben dem gewählten Dienst - "Entire Feature will be unavailable"
5) Klicken auf "Next" - "Change" - "Finish", um die Deinstallation abzuschließen.

Nach einem Neustart wird der jeweilige Dienst deinstalliert und sämtliche Einstellungen zurückgesetzt.

KEBA © KEBA 2021

8.9.2 Whitelisting über AppLocker

Der Applocker blockiert die Ausführung von Programmen, Skripten und Installationsprogrammen, wenn diese nicht in einer Liste (Whitelist) registriert und mit Ausführungsregeln hinterlegt sind.

Diese Regeln werden für die Benutzer (ausgenommen Admins) in den Standardeinstellungen festgelegt.

Für folgende Ordner sind standardmäßig Ausnahmen festgelegt:

- %ProgramFiles%
- %ProgramFiles(x86%)
- Windows Ordner

Die Standardkonfiguration erlaubt dem Standardbenutzer die Ausführung von Programmen aus den ausgenommenen Verzeichnissen. Administratoren können hingegen alle Programme ausführen.

Die Konfiguration des AppLockers kann nach der Installation mittels Local Security Policy (secpol.msc) angepasst werden.

Weitere Informationen zur Konfiguration, sowie eine detaillierte Beschreibung des AppLockers sind auf der Homepage von Microsoft© ersichtlich.

8.9.3 Kiosk Desktop

Mittels Kiosk Desktop kann der Benutzerzugriff auf das Gerät eingeschränkt werden. Dies kann z.B. als Schutz vor Fehlbedienung dienen.

Um den Kiosk Desktop zu konfigurieren, wird der Kiosk Configurator verwendet. Dieser liegt nach der Installation als Verknüpfung am Desktop.

Information

Nach erfolgter Konfiguration wird der Kiosk Desktop immer nach dem Starten des Geräts angezeigt.

Kiosk Configurator

Die Oberfläche des Kiosk Configurators besteht aus folgenden Registerkarten:

- Settings: Optische Anpassungen vornehmen
- Shortcuts: Verknüpfungen bearbeiten
- Blocked keys: Gesperrte Tasten (-Kombinationen) festlegen
- Colors: Hintergrund- und Schriftfarbe einstellen
- Dock: Verknüpfungen auf der Taskleiste bearbeiten
- Action: Neustart, Import, Export

© KEBA 2021

Settings

Unter "Settings" können die Grafiken für Logo, Kopf- und Fußzeile ausgetauscht und die Positionen der Verknüpfungen konfiguriert werden.

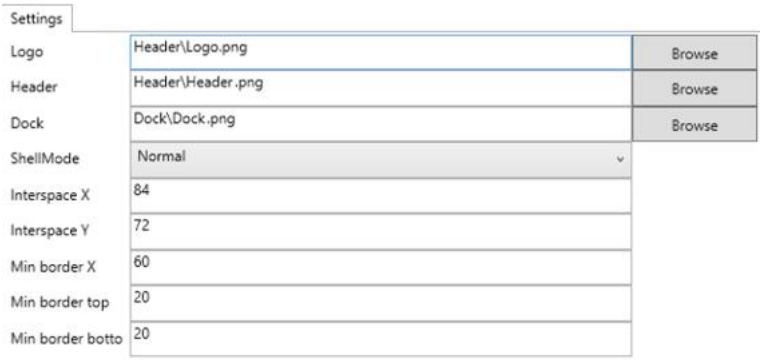


Abb. 8-90: Registerkarte "Settings"

Name	Beschreibung
Logo	Logografik rechts oben über "Browse" einfügen
Header	Grafik in Kopfzeile über "Browse" einfügen
Dock	Grafik in Fußzeile über "Browse" einfügen
Shell Mode	Ebene des Kiosk Desktops (im Drop-down-Menü wählbar)
Interspace X	X-Abstand zwischen den Verknüpfungen
Interspace Y	Y-Abstand zwischen den Verknüpfungen
Min border X	Mindestabstand zu den Rändern
Min border top	Mindestabstand nach oben
Min border bottom	Mindestabstand nach unten

Shortcuts

Unter "Shortcuts" können die Verknüpfungen angelegt und verwaltet werden.

In der linken Spalte sind alle angelegten Verknüpfungen aufgelistet. Angelegt werden diese mittels "New file" und "New dir".

In der rechten Spalte sind die Verknüpfungen aufgelistet, welche am Desktop aufscheinen.

Wird einer Verknüpfung eine Grafik für den normalen Anzeigezustand und eine Grafik für den gedrückten Zustand hinterlegt, so wird die Verknüpfung sofort aktiv gesetzt und ist am Kiosk Desktop sichtbar.

Die Reihenfolge der Elemente kann mit "▲" und "▼" angepasst werden.

KEBA © KEBA 2021

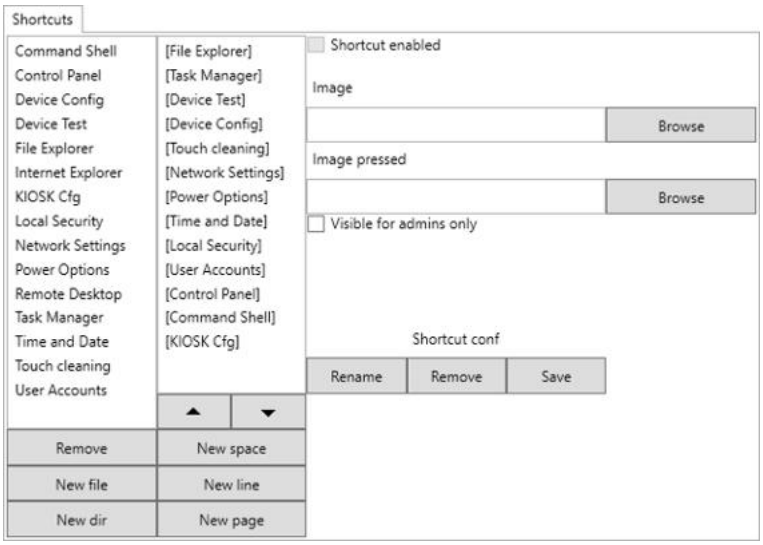


Abb. 8-91: Registerkarte "Shortcuts"

Name	Beschreibung
Remove	Löschen der Verknüpfung
New file	Neue Datei-Verknüpfung anlegen
New dir	Neue Ordner-Verknüpfung anlegen
▲	Selektiertes Element nach oben (vor) verschieben
▼	Selektiertes Element nach unten (hinten) verschieben
New space	Leeren Platzhalter einfügen
New line	Neue Zeile beginnen
New page	Neue Seite beginnen
Shortcut enabled	Verknüpfung ist aktiv (wird automatisch gesetzt, wenn beide Grafiken hinterlegt sind)
Image	Grafik über "Browse" einfügen
Image pressed	Grafik für gedrückten Zustand über "Browse" einfügen
Visible for admins only	Verknüpfung nur für Admins sichtbar
Rename	Umbenennen der Verknüpfung
Remove	Löschen der Verknüpfung
Save	Speichern der Konfiguration

Blocked keys

Unter "Blocked keys" können Tasten und Tastenkombinationen gesperrt werden.

In der linken Spalte werden die Elemente angezeigt (maximal 8), denen gesperrte Tasten hinzugefügt werden können. In der rechten Spalte werden jeweils die hinzugefügten (gesperrten) Tasten angezeigt.

© KEBA 2021

Durch Selektion eines der Elemente aus der linken Spalte können die gesperrten Tasten im Drop-down-Menü ausgewählt und über "Add key" dem Element hinzugefügt werden.

Abb. 8-92: Registerkarte "Blocked Keys"

Name	Beschreibung
Key	Drop-down-Menü mit allen verfügbaren Tasten
Add key	Gewählte Taste sperren
Remove keys	Gewählte Taste entfernen

Colors

Unter "Colors" können die Farben des Kiosk Desktop angepasst werden.

Mittels "Select" kann die gewünschte Farbe ausgewählt werden. In den farbigen Feldern werden die RGB-Werte der gewählten Farbe angezeigt.

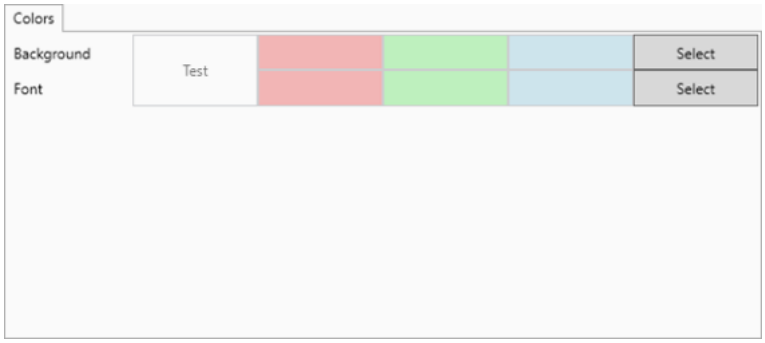


Abb. 8-93: Registerkarte "Colors"

Name	Beschreibung
Background	Hintergrundfarbe
Font	Schriftfarbe

© KEBA 2021

Dock

Unter "Dock" können bestimmte Funktionen an die Taskleiste angeheftet werden.

Herunterfahren, Neustarten, Task-Übersicht, Sperren, Abmelden und Tastatur (On Screen Keyboard).

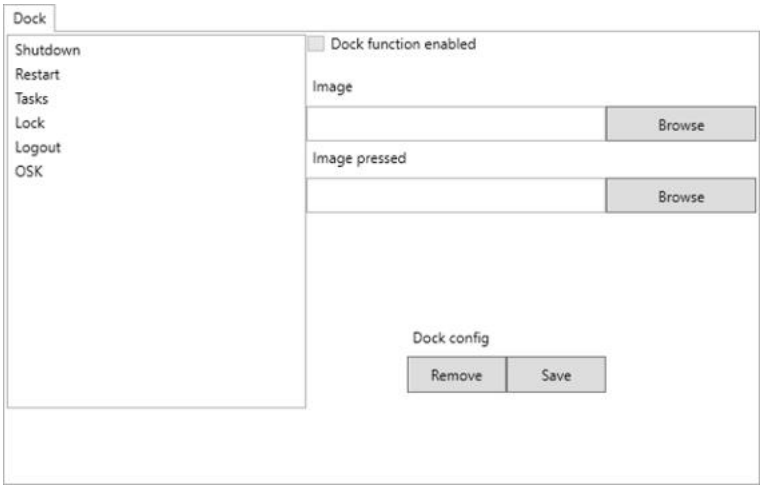


Abb. 8-94: Registerkarte "Dock"

Name	Beschreibung
Image	Grafik über "Browse" einfügen
Image pressed	Grafik für gedrückten Zustand über "Browse" einfügen
Remove	Entfernen der Funktion
Save	Speichern der Funktion

Action

Unter "Action" kann der Kiosk Desktop als Start-Anwendung (Active shell) festgelegt, neu gestartet oder die Konfiguration exportiert und importiert werden.

© KEBA 2021

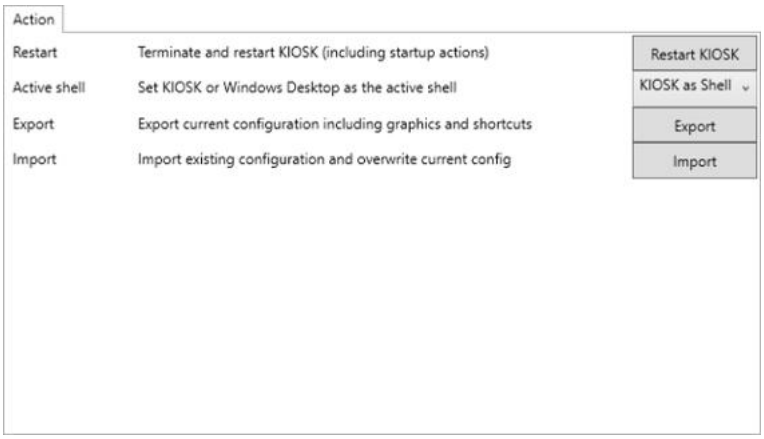


Abb. 8-95: Registerkarte "Action"

Name	Beschreibung
Restart	Startet den Kiosk Desktop neu Änderungen an der Konfiguration werden erst nach dem Neustart sichtbar
Active shell	
• KIOSK by ShellLauncher	Kiosk Desktop wird bei Start automatisch ausgeführt (nur ab Windows 10 verfügbar) Alle Programme im Autostart werden ausgeführt. Nur in Rücksprache mit KEBA wählen.
• KIOSK as Shell	Kiosk Desktop wird bei Start ausgeführt (standardmäßig ausgewählt) Alle Programme im Autostart werden ausgeführt.
• Explorer	Deaktiviert den automatischen Start von Kiosk Desktop
Export	Export der Konfiguration (inkl. Kiosk Desktop-Ordner)
Import	Import einer Konfiguration

8.9.4 KEBA Write Filter

Durch die Installation dieser Funktion wird das Dateisystem durch den KeWF (KEBA Write Filter) geschützt.

Mit der Standardkonfiguration wird verhindert, dass Dateien mit folgenden Dateierweiterungen am Laufwerk C:\ erstellt, umbenannt oder gelöscht werden (Blacklist):

Blacklist

a - g	h - p	m - z
*.ahk	*.hta, *.htm, *.html	*.reg, *.rgs
*.bat, *.bin	*.inf, *.ins, *.inx, *.ipf, *.isp, *.isu	*.scr, *.sct, *.shb, *.shs, *.sys

© KEBA 2021

a - g	h - p	m - z
*.cmd, *.chm, *.com, *.cpl, *.crt	*.job, *.js, *.jse, *.jar	*.u3p, *.url
*.docm, *.dotm, *.dll	*.lnk	*.vb, *.vbe, *.vbs, *.vbscript
*.exe, *.ex_	*.msc, *.msi, *.msp, *.mst	*.ws, *.wsf, *.wsh
*.gadget	*.paf, *.pif, *.ps1, *.pyc, *.pyo, *.pnf	*.xml

Auf allen anderen Laufwerken können weiterhin Files mit den genannten Extensions erstellt, umbenannt und gelöscht werden.

In der Konfiguration können weitere Ausnahmen (Whitelist) und "Wildcards" festgelegt und zusätzliche Laufwerke geschützt werden. In der Standardkonfiguration gilt die Ausnahme für folgende Dateien: „pagefile.sys“ und „hiberfil.sys“

Beispiel: Es können zwar alle *.exe- und *.dll-Dateien über die "Blacklist" gesperrt, aber gleichzeitig die Pfade `C:\Kundenverzeichnis1\*.exe` und `C:\Kundenverzeichnis2\KundenLibrary.dll` über die "Whitelist" erlaubt werden.

Information

Für weitere Informationen zur Konfiguration des KeWF KEBA-Support kontaktieren.

8.10 Verbindungsprotokolle

Um Daten zwischen dem Handbediengerät und der Steuerung zu übertragen, muss ein Protokoll definiert sein. Folgende Protokolle werden unterstützt:

- KVC: Ein von KEBA in die Steuerung integriertes definiertes proprietäres Protokoll.
- Modbus: Offener Standard
- OPC UA: Offener Standard
- ADS: Standardprotokoll für Beckhoff-Geräte
- S7: Standardprotokoll für Siemens-Geräte

Im Auslieferzustand ist standardmäßig kein Protokoll aktiviert. Weiterführende Informationen können den jeweiligen Protokollbeschreibungen entnommen werden.

Die Verbindungsprotokolle ermöglichen es, folgende Inhalte vom Handbediengerät zur Steuerung zu übertragen:

- Übertragung von Zustandsänderungen von Tasten des Keypads oder von Bedienelementen
- Setzen und Lesen von LED-Zuständen

© KEBA 2021

- Steuerung des Handbediengeräts bzw. Transfer diverser Parameter

Information

Es ist möglich, unterschiedliche Verbindungsprotokolle für die einzelnen Übertragungen zu verwenden. Es wird empfohlen, nur ein Verbindungsprotokoll zu verwenden, da sich sonst die Protokolle gegenseitig stören.

Installation

Information

Das Windows-Plattform Driver Setup darf nur für die Installation eines Verbindungsprotokolls verwendet werden. Eine Installation eines anderen Geräts ist nicht zulässig und kann zu Störungen im Betrieb führen.

Um ein Verbindungsprotokoll zu installieren, gehen Sie wie folgt vor:

1) Aufruf des Setups über "Programme und Funktionen" - "WindowsPlatformDriverSetup".
2) Klicken auf "Next" - "Change".
3) Auswählen des gewünschten Protokolls.

Protokoll	Setup Name
KVC	`KEBA Virtual Channel`
Modbus	`ModbusItf`
OPC UA	`OPCUAItf`
ADS	`ADSItf`
S7	`S7Itf`

4) Klicken auf den schwarzen Auswahlpfeil neben dem ausgewählten Protokoll.
5) Auswählen von "Entire Feature will be installed on local hard drive".
6) Klicken auf "Next" - "Change" - "Finish", um die Installation abzuschließen.

Deinstallation

Um ein Verbindungsprotokoll zu deinstallieren, gehen Sie wie folgt vor:

1) Aufruf des Setups "Programme und Funktionen" - "WindowsPlatformDriverSetup".
2) Klicken auf "Next" - "Change".
3) Auswählen des zu deinstallierenden Protokolls.
4) Klicken auf den schwarzen Auswahlpfeil neben dem ausgewählten Protokoll.

© KEBA 2021

5) Auswählen von "Entire feature will be unavailable".
6) Klicken auf "Next" - "Change" - "Finish", um die Deinstallation abzuschließen.

8.11 Tastenmanagement

Für jede Taste gibt es einen vordefinierten Tastencode. Durch Key-Mapping ist es möglich, die vordefinierten Tastencodes zu ändern („manipulieren“) oder zu deaktivieren, damit diese nicht mehr im Windows ausgewertet werden.

Der PS/2 Code der entsprechenden Taste kann mithilfe des "DeviceTest-Tools" ermittelt werden.

Konfiguration Key-Mapping

Um den Tasten des Keypads am Handbediengerät eine Funktion (Ausgabe) zu geben, müssen zuerst die Tasten eingebunden werden. Gehen Sie dazu wie folgt vor:

1) Öffnen der Datei `WinKeyMapExample.cfg` im Verzeichnis `C:\ProgramData\KEBA Automation\keview\system` mit einem Editor.

> ***Information***
>
> *Das Verzeichnis `C:\ProgramData` ist standardmäßig verborgen und muss über die Anzeigeeinstellungen des Explorers sichtbar gemacht werden.*

2) Kopieren aller Einträge im Unterpunkt `[ScancodeMapping_Txxx_Standard]` oder `[ScancodeMapping_Txxx_Robotic]`.
3) Einfügen aller Einträge im Unterpunkt `[ScancodeMapping]`.

Danach kann den Tasten des Keypads die gewünschte Ausgabe wie folgt zugeordnet werden.

Keypad Taste = Keypad Tastencode*), Modifikator*), gewünschte Ausgabe, gewünschter Modifikator

*) Diese Einstellung darf nicht verändert werden.

Beispiel:

```
KEY_001 = 00,20, 00,00,00,00,00,00, 00,3B, 00,2A,00,00,00,00
```

Anschließend muss die Datei als `KeyMap.cfg` gespeichert werden, um die Änderungen zu übernehmen. Datum und Uhrzeit werden automatisch (nach kurzer Zeit) an den Dateinamen angehängt.

Eine Liste der verfügbaren Tastencodes und Modifizierer für die Ausgabe befindet sich im nachfolgenden Kapitel.

Tastenfunktionen unterdrücken

Um alle Tastenfunktionen zu unterdrücken, gehen Sie wie folgt vor:

© KEBA 2021

1) Öffnen der Datei `WinKeyMapExample.cfg`
2) Im Unterpunkt `[Settings]` folgenden Parameter auf 1 setzen: `DropAllKeys=1`
3) Abspeichern der Datei als `KeyMap.cfg` im Verzeichnis `C:\ProgramData\KEBA Automation\keview\system`. Datum und Uhrzeit werden automatisch (nach kurzer Zeit) an den Dateinamen angehängt.

8.11.1 Tastencodes

Die folgenden Tabellen enthalten die zur Verfügung stehenden PS/2 Codes (Set 1) in Hexadezimal Schreibweise.

Modifikatoren

Taste	PS/2 Code	Taste	PS/2 Code
Strg links	00 1D	Strg rechts	E0 1D
Umschalttaste links	00 2A	Umschalttaste rechts	00 36
Alt links	00 38	Alt rechts	E0 38
Windowstaste links	E0 5B	Windowstaste rechts	E0 5C

Tasten (bezogen auf ein englisches Tastaturlayout)

Taste	PS/2 Code	Taste	PS/2 Code
' "	00 28	Nummernblock -	00 4A
, <	00 33	Nummernblock . Entf	00 53
- _	00 0C	Nummernblock /	E0 35
. >	00 34	Nummernblock 0 Einfg	00 52
/ ?	00 35	Nummernblock 1 Ende	00 4F
0)	00 0B	Nummernblock 2 abwärts	00 50
1 !	00 02	Nummernblock 3 Bild ab	00 51
2 @	00 03	Nummernblock 4 links	00 4B
3 #	00 04	Nummernblock 5	00 4C
4 $	00 05	Nummernblock 6 rechts	00 4D
5 %	00 06	Nummernblock 7 Pos1	00 47
6 ^	00 07	Nummernblock 8 aufwärts	00 48
7 &	00 08	Nummernblock 9 Bild auf	00 49
8 *	00 09	Nummernblock =	00 59
9 (	00 0A	Nummernblock Enter	E0 1C
; :	00 27	Num Lock	00 45
= +	00 0D	Bild ab	E0 51
Pfeil abwärts	E0 50	Bild auf	E0 49
Pfeil links	E0 4B	Druck S-Abf	E0 37
Pfeil rechts	E0 4D	Enter	00 1C
Pfeil aufwärts	E0 48	Rollen	00 46

KEBA © KEBA 2021

Taste	PS/2 Code	Taste	PS/2 Code
Backspace	00 0E	Leertaste	00 39
Feststelltaste	00 3A	Tabulator	00 0F
Entf	E0 53	[{	00 1A
Ende	E0 4F	\ |	00 2B
Esc	00 01	] }	00 1B
F1	00 3B	` ~	00 29
F2	00 3C	a A	00 1E
F3	00 3D	b B	00 30
F4	00 3E	c C	00 2E
F5	00 3F	d D	00 20
F6	00 40	e E	00 12
F7	00 41	f F	00 21
F8	00 42	g G	00 22
F9	00 43	h H	00 23
F10	00 44	i I	00 17
F11	00 57	j J	00 24
F12	00 58	k K	00 25
F13	00 64	l L	00 26
F14	00 65	m M	00 32
F15	00 66	n N	00 31
F16	00 67	o O	00 18
F17	00 68	p P	00 19
F18	00 69	q Q	00 10
F19	00 6A	r R	00 13
F20	00 6B	s S	00 1F
F21	00 6C	t T	00 14
F22	00 6D	u U	00 16
F23	00 6E	v V	00 2F
F24	00 76	w W	00 11
Pos1	E0 47	x X	00 2D
Einfg	E0 52	y Y	00 15
Nummernblock *	00 37	z Z	00 2C
Nummernblock +	00 4E		

© KEBA 2021

8.12 Windows Einstellungen

Tastaturlayout

Standardmäßig ist am Handbediengerät das englische Tastaturlayout eingestellt. Der Benutzer kann über die Systemsteuerung neue Tastaturlayouts hinzufügen bzw. die primäre Sprache auswählen. Für Details zu den Einstellungen siehe Microsoft© Website.

Windows Aktivierung

WES7

Das KeTop mit WES7 wird bereits lizensiert und aktiviert ausgeliefert.

Windows 10

Das KeTop wird mit einer gültigen Lizenz und einer verzögerten Aktivierung ("deferred activation") ausgeliefert. Ein Produktschlüssel vom Typ Embedded Product Key Entry Activation (ePKEA) ist integriert. Sobald das KeTop mit dem Internet verbunden wird, erfolgt die Aktivierung automatisch. Wenn das Gerät nie mit dem Internet verbunden wird, bleibt es im Zustand der verzögerten Aktivierung. Sollte die Aktivierung fehlschlagen und das Gerät in den Zustand "nicht aktiviert" übergehen, kontaktieren Sie bitte KEBA.

Für weiterführende Informationen siehe Microsoft© Website.

AutoLogon

Mit aktiviertem AutoLogon wird nach dem Hochlauf am Handbediengerät kein Anmeldeschirm ("logon screen") angezeigt, sondern automatisch der eingestellte Benutzer eingeloggt. Es muss kein Passwort eingegeben werden.

Information

Vollständiger Hochlauf nicht mehr möglich!

Wenn der AutoLogon aktiviert ist, dürfen Benutzer, Benutzerpasswort und Domain-Name nicht verändert werden. Um diese Einstellungen zu verändern, muss der AutoLogon deaktiviert sein.

AutoLogon unterbrechen

Um den automatischen Logon einmalig zu unterbrechen, muss eine der Umschalttasten gedrückt und gehalten werden, bevor Windows den konfigurierten Benutzer automatisch anmeldet.

Schreibschutz für Speichermedien

WES7

Ein Schreibschutz für den Speicher kann mittels Enhanced Write Filter (EWF) realisiert werden.

KEBA © KEBA 2021

Windows 10

Ein Schreibschutz für den Speicher kann mittels Unified Write Filter (UWF) realisiert werden.

Weiterführende Informationen siehe Microsoft© Website.

Windowstaste

Die Power-Taste ⏻ entspricht der Windows Powertaste und kann dementsprechend belegt werden. Weitere Details zur Belegung siehe Microsoft© Website.

Microsoft Edge installieren

Über das Setup "WindowsCustomizingSetup" kann Microsoft Edge installiert und als Standardbrowser eingereichtet werden. Gehen Sie dazu wie folgt vor:

1) Aufruf des Setups über "Programme und Funktionen" - "WindowsCustomizingSetup".
2) Klicken auf "Change".
3) Auswählen von "Microsoft Edge".
4) Klicken auf den schwarzen Auswahlpfeil neben dem ausgewählten Dienst.
5) Auswählen von "Entire Feature will be installed on local hard drive".
6) Klicken auf "Next" - "Change" - "Finish", um die Installation abzuschließen.

Zusätzliche Chiffren aktivieren

Über das Setup "WindowsCustomizingSetup" können zusätzliche Chiffren aktiviert werden, die für WinCC benötigt werden. Gehen Sie dazu wie folgt vor:

1) Aufruf des Setups über "Programme und Funktionen" - "WindowsCustomizingSetup".
2) Klicken auf "Change".
3) Auswählen von "Additional ciphers activation".
4) Klicken auf den schwarzen Auswahlpfeil neben dem ausgewählten Dienst.
5) Auswählen von "Entire Feature will be installed on local hard drive".
6) Klicken auf "Next" - "Change" - "Finish", um die Installation abzuschließen.

© KEBA 2021

8.13 Programmierung

HWApi

Am Handbediengerät gibt es die Programmierschnittstelle HWApi, über die die Bedienelemente und Tastatur angesprochen und HW-Eigenschaften abgefragt werden können. Um die Programmierschnittstelle HWApi verwenden zu können, wird die Programmierumgebung HWApiSDK benötigt. Diese kann bei KEBA auf Anfrage bezogen werden.

Für weitere Informationen kontaktieren Sie bitte KEBA.

KEBA © KEBA 2021

9 Betrieb und Bedienung

9.1 Hochlauf

Der Hochlauf- bzw. Startvorgang des Handbediengeräts nach dem Drücken der Power-Taste kann am Bildschirm mitverfolgt werden und verläuft in folgender Reihenfolge:

1) Anzeige des Boot-Splashscreen
2) Laden und Starten des Betriebssystems. Dieser Vorgang kann bis zu 3 Minuten dauern. Währenddessen wird ein schwarzer Bildschirm angezeigt.
3) Logindialog (nicht angezeigt, wenn Autologon aktiviert)
4) Windows-Desktop wird gestartet

Beim ersten Anmelden mit dem Administrator-Benutzer "keba" muss kein Passwort eingegeben werden. Unmittelbar nach der ersten Anmeldung muss ein Passwort vergeben werden. Hierfür folgen Sie bitte den Anweisungen am Bildschirm.

Achtung

Ein Flash-Speichermedium ermöglicht eine begrenzte Anzahl von Schreibzyklen. Wird diese überschritten, besteht die Gefahr eines Hardwaredefekts. Es wird daher empfohlen, für zyklische Schreibvorgänge ein wechselbares Speichermedium zu verwenden.

Standardbenutzer

Am Gerät stehen folgende Standardbenutzer zur Verfügung:

- keba: Dieser Benutzer besitzt **Administratorrechte** und kann Systemänderungen vornehmen und Software installieren.
- operator: Dieser Benutzer besitzt **Standardrechte** und ist für den normalen Betrieb ohne administrative Berechtigungen vorgesehen.

Es wird empfohlen, unmittelbar nach der ersten Anmeldung für alle Benutzer ein anderes Passwort zu vergeben, um das System vor unautorisierten Zugriffen zu schützen. Dazu folgen Sie bitte den Anweisungen am Bildschirm.

Information

Im Standardbetrieb wird die Verwendung des Benutzers "operator" empfohlen, um eine Systemsicherheit zu gewährleisten.

© KEBA 2021

9.2 Ausschalten des KeTops

Das Gerät kann z.B. über **Start ► Herunterfahren** heruntergefahren werden. Für die Ausschaltsicherheit des KeTops können entsprechende Konzepte vorgesehen werden (z.B. UWF Schreibfilter, ...).

Power-Taste

Durch Drücken der Power-Taste ⏻, wechselt das KeTop standardmäßig in den Hibernation-Modus. Die Funktion der Power-Taste kann über **Start ► Systemsteuerung ► Energieoptionen** konfiguriert werden.

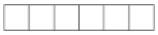
Achtung

Die Power-Taste ist standardmäßig so konfiguriert, dass bei Betätigen (und gedrückt halten) nach 5 Sekunden eine Spannungstrennung des Geräts erfolgt. In diesem Fall gehen alle Daten im Arbeitsspeicher des Geräts verloren.

9.3 Betriebszustände Basisstation

Dieses Kapitel beschreibt die möglichen Betriebszustände der Basisstation.

Der aktuell aktive Betriebszustand wird über den LED-Status-Balken (bzw. externe Signalsäule) angezeigt.

Anzeige	Betriebszustand	Beschreibung
Grün	Normal	Das Handbediengerät ist korrekt verbunden und der Not-Halt nicht betätigt. Die Not-Halt Ausgänge der Basisstation sind im selben Zustand wie der Not-Halt des Handbediengeräts.
Weiß 	Bridge active	Das Handbediengerät ist nicht verbunden, die Not-Halt Ausgänge der Basisstation sind geschlossen, es liegt kein ungültiger Zustand, Fehler oder betätigter Not-Halt vor Abmelden des Handbediengeräts vor.
Weiß blinkend	DIP-Switch nicht eingestellt	Der DIP-Switch an der Basisstation ist nicht eingestellt. Einstellen des DIP-Switches laut Tabelle im Kapitel "Bedienbereichs-Konfiguration".
Nacheinander erlöschende, gelbe LEDs	Paring/Unpairing timer	Es wurde ein Handbediengerät mit betätigtem Not-Halt verbunden. Wird innerhalb von ca. 10 Sekunden der Not-Halt entriegelt, wechselt die Basistation in einen gültigen Betriebsmodus. Wird die Zeit überschritten, geht die Basistation in den sicheren Zustand (die Ausgänge werden geöffnet).

KEBA © KEBA 2021

Anzeige	Betriebszustand	Beschreibung
Rot	Estop	Sicherer Zustand. Folgende Punkte können den sicheren Zustand auslösen: ● Der Not-Halt am Handbediengerät oder auf der Basisstation wurde ausgelöst. ● Der "Reset" Taster auf der Basisstation wurde gedrückt. Das Handbediengerät wurde damit von der Basisstation abgemeldet. Zum Quittieren muss der Not-Halt entriegelt werden.

9.4 Betriebsverhalten

Basisstation ausgeschaltet

Ist die Basisstation ausgeschaltet, werden die Relais der Not-Halt-Kreise nicht mehr aktiv zugehalten und dadurch ist der Not-Halt-Kreis geöffnet (vergleichbar mit betätigtem Not-Halt). Die Zustimmtaster-Ausgänge bleiben ebenfalls geöffnet.

Basisstation eingeschaltet

Wird die Basisstation eingeschaltet (mit Spannung versorgt), werden die Zustände der Eingänge und der letzte gespeicherte Not-Halt-Zustand abgefragt. Resultierend aus dieser Abfrage kann die Basisstation die definierten Betriebszustände annehmen. Die Zustimmtaster-Ausgänge bleiben geöffnet.

Betrieb mit verbundenem Handbediengerät

Nach dem erfolgreichen Anmelden eines Handbediengerät an der Basisstation folgen die Not-Halt-Relais-Ausgänge der Basisstation dem Zustand des Not-Halts am Handbediengeräts, sofern der Not-Halt der Basisstation nicht betätigt ist. Die Zustimmtaster-Ausgänge folgen dem Schaltelement am Handbediengerät.

Erst nach erfolgreichem Aufbau der sicheren Verbindung zwischen Handbediengerät und Basisstation wird der beleuchtete Not-Halt des Handbediengeräts wirksam. Führt ein Fehler in der Basisstation dazu, dass der Not-Halt auf dem Handbediengerät unwirksam wird, dem Bediener jedoch signalisiert wird, dass er aktiv ist, so werden die Zustimmtaster-Ausgänge und die Not-Halt-Ausgänge geöffnet.

Wird die Basisstation bei verbundenem Handbediengerät ausgeschaltet, wird am Handbediengerät eine Fehlermeldung ausgegeben. Das Handbediengerät muss neu gestartet werden, um wieder einen korrekten Betrieb (nicht verbunden) zu ermöglichen.

© KEBA 2021

Betrieb mit abgemeldetem Handbediengerät

Wird ein Handbediengerät abgemeldet, so wird der darauf befindliche beleuchte Not-Halt inaktiv und der Zustimmtaster nicht mehr funktionsfähig. Da jedoch ein abgemeldeter inaktiver Not-Halt nicht zu einem Auslösen der Sicherheitsfunktion "Not-Halt" führt, bleiben die Not-Halt-Kreise der Basisstation weiterhin geschlossen. Somit wird der Not-Halt-Ausgang (Relais-Ausgang) der Basisstation nicht ausgelöst. Auch weitere, an der Maschine vorhandene Not-Halt, verlieren nicht ihre Wirkung.

Bei einer störungs- oder fehlerbedingten Unterbrechung der sicheren Verbindung zwischen Handbediengerät und Basisstation wird der Not-Halt an der Basisstation automatisch ausgelöst.

Ein auf der Basisstation ausgelöster Not-Halt wird durch das Abmelden des Handbediengeräts nicht aufgehoben.

Handbediengerät an-/abmelden

Ist an der Basisstation ein Handbediengerät verbunden (angemeldet) und soll ein anderes Handbediengerät angemeldet werden, muss zuerst das aktuell angemeldete Gerät abgemeldet ("unpair") werden. (Siehe 11 Verbinden mit Basisstation.)

Der beleuchtete Not-Halt am verbundenem Handbediengerät wird nach erfolgreicher Anmeldung an der Basisstation aktiviert.

Wird ein Handbediengerät mit betätigtem Not-Halt verbunden, kann dieser innerhalb von 10 Sekunden entriegelt werden, ohne dass ein Not-Halt ausgelöst wird. Wird der Not-Halt nicht innerhalb von 10 Sekunden entriegelt, wird ein Not-Halt ausgelöst.

Windows Betriebssystem am Handbediengerät

m Auslieferzustand ist die Windows Firewall aktiviert und durch eine "Inbound" Regel werden alle eingehenden Anfragen blockiert. Falls für die Kommunikation Ports und Services benötigt werden, müssen diese in der Firewall mit Regel ausgenommen werden. Für Dienste die mit Hilfe der einzelnen Setups aktiviert werden, wird in der Firewall eine Regel hinzugefügt. Wird eine zusätzliche Regel hinzugefügt, müssen die Konsequenzen bewusst sein und liegen nicht mehr in der Verantwortung von KEBA.

9.5 Ladeverhalten des Akkus

Der Akku kann mittels mitgelieferter Ladestation oder optional mittels Netzteil geladen werden.

Laden bei hohen Umgebungstemperaturen

Rechenintensive Applikationen bei hohen Umgebungstemparaturen können während des Ladens zu hohen Temperaturen des Akkus führen.

KEBA © KEBA 2021

Wenn die Umgebungstemperatur 45°C übersteigt, wird das Laden des Akkus unterbrochen. Der Ladevorgang wird fortgesetzt, sobald die Temperatur des Akkus wieder unter 40°C fällt.

Folgende Maßnahmen werden zur Abkühlung des Akkus empfohlen:

- Gerät in eine Umgebung mit geringerer Temperatur (< 25°C) bringen.
- Gerät für eine gewisse Zeit ausschalten oder in den Ruhezustand versetzten.

9.6 "System State" Anzeige

Wird ein Zusatz-Akku (siehe 17.6 Zubehör) angesteckt, erscheint im "System Tray" der Taskleiste das Icon der "System State" Anzeige. Durch Klick darauf oder durch Drücken des Ident-Tasters am Handbediengerät für min. 3 s, öffnet sich folgender Dialog:

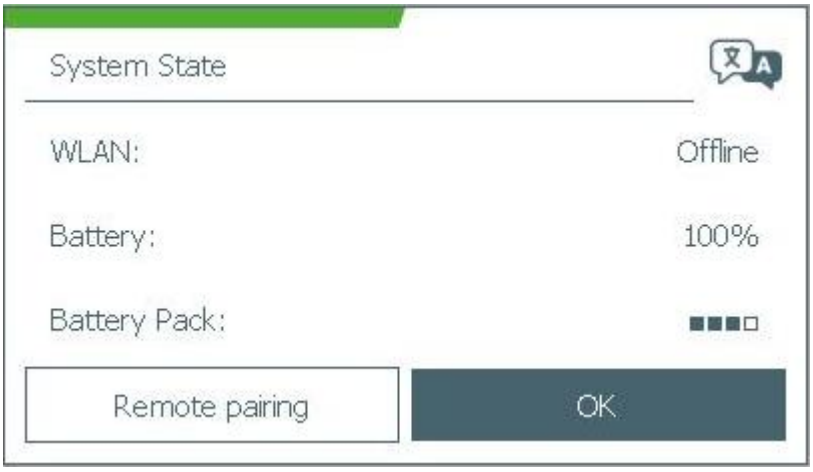


Abb. 9-96: "System State" Anzeige

Anzeige	Beschreibung
WLAN:	WLAN Verbindung
Battery:	Zustand des internen Akkus
Battery Pack:	Zustand des Zusatz-Akkus
Remote paring:	Herstellen einer sicheren Verbindung (siehe 11 Verbinden mit Basisstation)
OK	Schließen des Dialogs

© KEBA 2021

10 Validierung

Nachdem die Basisstation verkabelt, montiert und konfiguriert wurde, müssen folgende Funktionen geprüft und dokumentiert werden:

- Betätigung des Not-Halt eines angeschlossenen Handbediengeräts
- Betätigen und Testen der Schaltelemente, speziell den Zustimmtaster und den Schlüsselschalter
- Durchführung und Überprüfung des gesamten An- und Abmeldevorgangs des Handbediengeräts an der Basisstation ("Pairing"/"Unpairing")
- Sofern es für die Applikation relevant ist, Durchführung und Überprüfung eines Remote-An- und Abmeldevorgangs des Handbediengeräts an der Basisstation ("Remote Pairing"/"Remote Unparing")
- Prüfung aller Sicherheitsfunktionen (mindestens Not-Halt und Zustimmtaster)
- Überprüfung der Sichtbarkeit/Erkennbarkeit des beleuchteten Not-Halts sowie des LED-Balkens und der Signalsäule

Information

Für die Validierung muss sich die Maschine in einem sicheren Zustand befinden. Der Gefahrenbereich muss frei sein.

10.1 Validierung der Abstandsmessung

Um die Abstandsmessung zwischen mobilem Handbediengerät und Basisstation anzuzeigen, gehen Sie wie folgt vor:

- Durchführen des Standard-Pairings von Handbediengerät mit der Basisstation.
- Drücken des "Ident"-Tasters für 3 Sekunden um den Dialog "System State" zu öffnen.
- Ausrichten des Handbediengerätes mit direktem Sichtkontakt zur Basisstation.
- Bewegen des Handbediengerätes an die Grenze des Arbeitsbereiches.
- Überprüfen, ob die Nothaltbeleuchtung bei erwartetem Abstandswert pulsiert.
- Ablesen des angezeigten Abstandswerts.

Der angezeigte Abstandswert muss dem tatsächlichen Abstand, mit einer Toleranz von +/- 1 m entsprechen.

KEBA © KEBA 2021

11 Verbinden mit Basisstation

Um eine Verbindung mit der Basisstation herzustellen, muss zwischen Handbediengerät und Basisstation ein sogenanntes "pairing" durchgeführt werden. Es kann immer nur ein Handbediengerät mit einer Basisstation verbunden sein. Erst nach erfolgreichem "pairing" können die notwendigen Konfigurationseinstellungen der Basisstation durchgeführt werden (siehe 8.4.1 Basestation).

Der beleuchtete Not-Halt funktioniert nur, wenn eine korrekte Verbindung zur Basisstation vorhanden ist. Die Übertragung der sicheren Daten erfolgt über Bluetooth, die funktionalen Daten über WLAN. Wird die Bluetooth Verbindung unterbrochen, leuchtet der Not-Halt nicht mehr und ist damit nicht verfügbar. Bei jedem Verbindungsabbruch (z. B. durch Überschreiten des höchstzulässigen Abstandes zur Basisstation), bleiben die Geräte weiterhin gepairt. Eine Datenübertragung ist jedoch nur mehr über WLAN (oder abhängig der Entfernung nicht mehr) möglich.

Befindet sich das Handbediengerät erneut im Funkbereich der Basisstation, wird automatisch wieder eine sichere Bluetooth-Verbindung zur ursprünglich verbundenen (gepairten) Basisstation aufgebaut. Um das Handbediengerät mit einer anderen Basisstation zu verbinden, muss das Handbediengerät zuerst von der ursprünglich verbunden (gepairten) Basistation getrennt werden.

Basisstation verbinden (Pairing)

Um die sichere Verbindung herzustellen ("pair"), gehen Sie wie folgt vor:

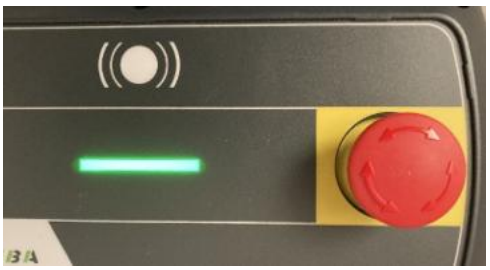
1) Handbediengerät an die gewünschte Basisstation halten (max. Entfernung 2 cm).
2) Bei Erkennen der Basisstation vibriert das Gerät und ein Dialog öffnet sich automatisch, der die Seriennummer oder den Namen der Basisstation anzeigt.
3) Bestätigen mit "Yes".

Die sichere Verbindung ist hergestellt. Eine erfolgreich hergestellte Verbindung ist am Beleuchtungs-Zustand des LED-Balkens der Basisstation und des Not-Halts des Handbediengeräts erkennbar. Dies ist mit einer visuellen Kontrolle zu verifizieren.

Information

Ist die optionale Bedienbereichsüberwachung konfiguriert, muss sich der Anwender bis zum Abschluss des Pairingvorganges in unmittelbarer Nähe der Basisstation befinden. Ansonsten kann dies zu ungewolltem Stillsetzen der Maschine führen.

© KEBA 2021

Basisstation verbunden	Handbediengerät verbunden
	

Je nach eingestellter Konfiguration verbindet sich das Handbediengerät für den funktionalen Datenaustausch automatisch mit der Basisstation oder dem Hallennetzwerk.

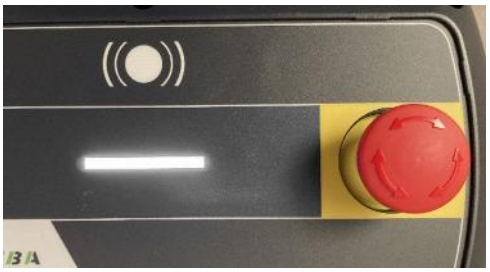
Nach Beenden der Arbeiten muss die sichere Verbindung durch ein sogenanntes "unpairing" wieder freigegeben werden.

Basisstation trennen (Unpairing)

Um die sichere Verbindung zu trennen ("unpair"), gehen Sie wie folgt vor:

1) Handbediengerät an die gewünschte Basisstation halten (max. Entfernung 2 cm).
2) Das Gerät vibriert und ein Dialog öffnet sich automatisch, der die Seriennummer oder den Namen der Basisstation anzeigt.
3) Bestätigen mit "Yes".

Die sichere Verbindung ist getrennt. Eine erfolgreich getrennte Verbindung ist am Beleuchtungs-Zustand des LED-Balkens der Basisstation und des Not-Halts des Handbediengeräts erkennbar. Dies ist mit einer visuellen Kontrolle zu verifizieren.

Basisstation getrennt	Handbediengerät getrennt
	

Je nach eingestellter Konfiguration verbindet sich das Handbediengerät für den funktionalen Datenaustausch automatisch mit dem Hallennetzwerk oder bleibt offline.

KEBA © KEBA 2021

Remote Pairing / Unpairing

WARNUNG!

Es muss sichergestellt werden, dass sich während eines "Remote Pairing" Vorgangs ein fix verdrahteter Not-Halt in der Nähe des Benutzers befindet!

Ist es in Sonderbetriebsarten oder gewissen Zuständen nicht möglich, das Handbediengerät direkt an die Basisstation zu halten, ist die Funktion "Remote Pairing" erforderlich. Dazu muss jedoch eine Sichtverbindung zur gewünschten Basisstation bestehen, um sicherzustellen, sich mit der tatsächlich gewünschten Basisstation zu verbinden.

Information

Bevor ein "Remote Pairing" durchgeführt werden kann, muss zwischen Handbediengerät und Basisstation einmal ein "pairing" mit anschließender Grundkonfiguration erfolgt sein.

Es wird empfohlen, ein Handbediengerät mit allen Basisstationen einer Halle einmal zu verbinden, um eine Liste aller Basisstationen zu erstellen (siehe Kapitel 8.4.1 Basestation). Diese Liste kann durch "Export" am ursprünglichen Handbediengerät und "Import" auf allen weiteren Handbediengeräten übertragen werden, um damit das Remote Pairing/Unpairing zu erleichtern.

Remote Pairing

Um die sichere Verbindung herzustellen, ohne das Handbediengerät direkt an die Basisstation zu halten, gehen Sie wie folgt vor:

1) Ident-Taster am Handbediengerät mind. 3 s drücken.
2) Dialog "System State" öffnet sich.

Abb. 11-97: Dialog "System State"

3) Drücken von "Remote pairing" und Eingabe des Passworts.

© KEBA 2021

4) Eingabe der MAC-Adresse der gewünschten Basisstation. Alternativ dazu kann aus der abgespeicherten Liste der Basisstationen über den Namen ausgewählt werden.

5) Auswahl des LED-Musters, welches an der gewünschten Basisstation zu diesem Zeitpunkt angezeigt wird.

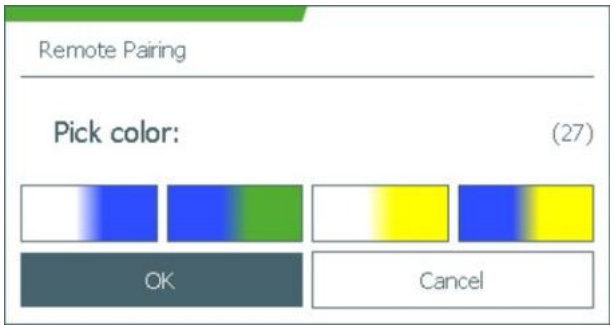


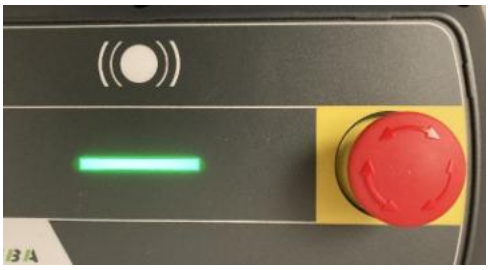
Abb. 11-98: Dialog LED-Muster

6) Bestätigen mit "OK".

Die sichere Verbindung ist hergestellt. Eine erfolgreich hergestellte Verbindung ist am Beleuchtungs-Zustand des LED-Balkens der Basisstation und des Not-Halts des Handbediengeräts erkennbar. Dies ist mit einer visuellen Kontrolle zu verifizieren.

Information

Wird Remote Pairing außerhalb des definierten Bedienbereichs durchgeführt, reagiert die Bedienbereichsüberwachung sofort mit den Maßnahmen des Übertretungsbereichs. Der Not-Halt wird ausgelöst und die Maschine geht in sicheren Zustand.

Basisstation verbunden	Handbediengerät verbunden
	

Je nach eingestellter Konfiguration verbindet sich das Handbediengerät für den funktionalen Datenaustausch automatisch mit der Basisstation oder dem Hallennetzwerk.

Remote Unpairing

Um die sichere Verbindung zu trennen, ohne das Handbediengerät direkt an die Basisstation zu halten, gehen Sie wie folgt vor:

1) Ident-Taster am Handbediengerät mind. 3 s drücken.

KEBA © KEBA 2021

2) Dialog "System State" öffnet sich.

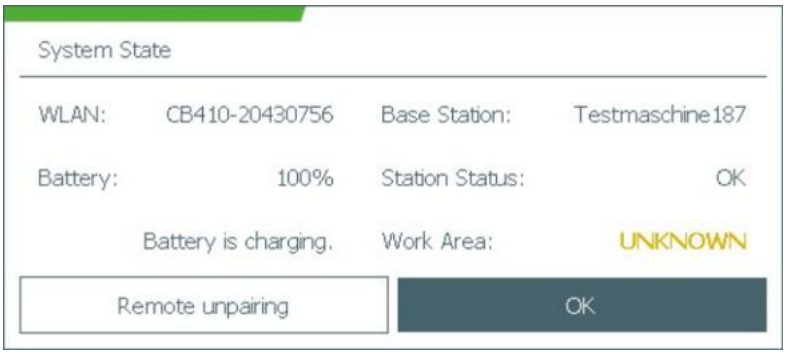


Abb. 11-99: Dialog "System State"

3) Drücken von "Remote unpairing" und Eingabe des Passworts.

4) Auswahl des LED-Musters, welches an der gewünschten Basisstation zu diesem Zeitpunkt angezeigt wird.

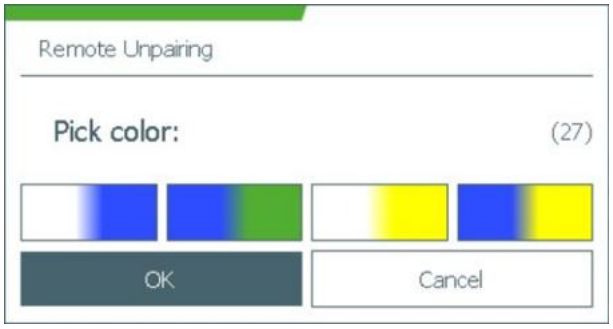
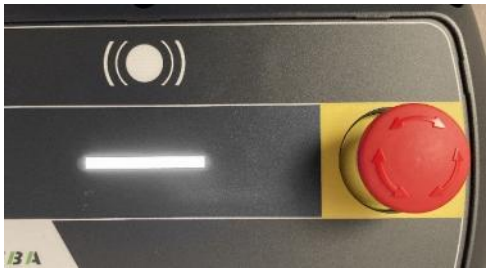


Abb. 11-100: Dialog LED-Muster

5) Bestätigen mit "OK".

Die sichere Verbindung ist getrennt. Eine erfolgreich getrennte Verbindung ist am Beleuchtungs-Zustand des LED-Balkens der Basisstation und des Not-Halts des Handbediengeräts erkennbar. Dies ist mit einer visuellen Kontrolle zu verifizieren.

Basisstation getrennt	Handbediengerät getrennt
	

Je nach eingestellter Konfiguration verbindet sich das Handbediengerät für den funktionalen Datenaustausch automatisch mit dem Hallennetzwerk oder bleibt offline.

© KEBA 2021

Wichtig ist, dass eine solche Umschaltung von Automatik in Sonderbetrieb nur einmalig möglich ist! Für das Zurücksetzen von Sonderbetrieb in Automatik dürfen die Ausgänge "Pairing/Sonderpairing" nicht verwendet werden. Es muss entweder ein Schlüsselschalter oder eine andere Maßnahme verwendet werden.

KEBA © KEBA 2021

12 Diagnose

Dieses Kapitel beschreibt die möglichen Fehlerzustände und deren Behebung.

Information

Bei Verwendung der optionalen Bedienbereichsüberwachung ist die Quittierung eines Fehlers ausschließlich im Bedienbereich möglich.

Tritt ein Fehler auf, wird dies über den LED-Status-Balken an der Basisstation angezeigt.

Anzeige	Fehler	Behebung
Blau	Schwerer Fehler: LED des beleuchteten Not-Halts am angeschlossenen Handbediengerät defekt. Ein Not-Halt wird ausgelöst.	Der Fehler ist im laufenden Betrieb quittierbar. Beheben des Fehlers durch Austauschen des Handbediengeräts bzw. Verbinden eines Handbediengeräts mit funktionierender LED des beleuchteten Not-Halts.
Halb rot / halb blau	BBÜ-Fehler: Fehler bei der Bedienbereichsüberwachung	Verbindung zum Gerät trennen. Betätigen und Entriegeln des Not-Halts.
Gelb	Feldbus-Fehler (nur bei CB42x und CB43x): Es findet keine Feldbus Kommunikation statt. Die F-Adresse ist nicht korrekt eingestellt.	Einstellung der F-Adresse kontrollieren. Verbindung und Einstellung der Feldbusanbindung kontrollieren.
Gelb blinken	Feldbus-Fehler: Neustart der Basisstation oder des F-Host. Kommunikationsfehler zwischen Basisstation und F-Host. F-Host fordert den sicheren Zustand der Basisstation an.	Anwenderquittung am F-Host notwendig.
Halb gelb / halb rot blinken	Schwerer Fehler: Der mit blauen LEDs angezeigte Fehler wurde nicht behoben.	Der Fehler ist im laufenden Betrieb quittierbar. Verbinden eines Handbediengeräts mit funktionstüchtigem beleuchtetem Not-Halt.

© KEBA 2021

Anzeige	Fehler	Behebung
Halb gelb / halb rot blinken	Schwerer Fehler: Der Not-Halt wurde ausgelöst. Die Basisstation wurde stromlos gesetzt und der Not-Halt entriegelt. Beim erneuten Starten der Basisstation wird ein Fehler angezeigt und der Not-Halt erneut ausgelöst.	Der Fehler ist im laufenden Betrieb quittierbar. Betätigen und Entriegeln des Not-Halts.
Halb gelb / halb rot blinken	Schwerer Fehler: Die Not-Halt Kreise eines Schaltelements sind asynchron. Ein Not-Halt wird ausgelöst.	Der Fehler ist im laufenden Betrieb quittierbar. Betätigen und Entriegeln des betroffenen Not-Halts.
Halb gelb / halb rot blinken	Schwerer Fehler: Es wurde ein Verbindungsabbruch automatisch wiederhergestellt. Ein Not-Halt wird ausgelöst.	Der Fehler ist im laufenden Betrieb quittierbar. Betätigen und Entriegeln des Not-Halts.
Rot blinken	Fataler Fehler: Es wurde ein sicherheitskritischer Hardware-Fehler erkannt. Ein Not-Halt wird ausgelöst. Möglicher Fehler bei Auswahl der DIP-Switches für BBÜ-Einstellung oder Gateway-F-Adresse.	Der Fehler ist im laufenden Betrieb nicht quittierbar. Die Basisstation muss getauscht werden. Bitte befolgen Sie die Vorgehensweise zur Einstellung der BBÜ Grenzen (siehe 8.3 Bedienbereichs-Konfiguration (sicherheitsrelevant)) sowie zur Einstellung der Gateway-F-Adresse (siehe 8.2 F-Adressierung (nur bei CB42x und CB43x)).
Rotes Lauflicht	Verbindungsabbruch: Die Verbindung zum Handbediengerät wurde unterbrochen.	Verbindung zum Handbediengerät wieder herstellen.
Rot	Betätigter Not-Halt: Sicherer Zustand wurde ausgelöst.	Entriegeln des Not-Halts (siehe 9.3 Betriebszustände Basisstation).

Alle Fehler, die vom Handbediengerät ausgelöst werden, können nach dem Abmelden quittiert werden. Der LED-Balken der Basisstation leuchtet dann weiß.

KEBA © KEBA 2021

13 Instandhaltung

Die Basisstation ist wartungsfrei. Es dürfen keine etwaigen Reparaturen durchgeführt werden.

Beim Handbediengerät können folgende Tätigkeiten durchgeführt werden:

- Reinigen des Touchscreens
- Wechseln des Akkus
- Erstellen eines Statusreports
- Erstellen eines Backups
- Wiederherstellen eines Backups
- Tauschen der SD-Karte

13.1 Reinigung des Touchscreens

Achtung

Reinigen Sie den Touchscreen nie mit Lösungsmittel, Scheuermilch oder Scheuerschwämmen. Andernfalls kann es zur Beschädigung der Touchoberfläche kommen!

Verwenden Sie zur Reinigung ein weiches Tuch, das Sie leicht mit Wasser oder einem milden Reinigungsmittel angefeuchtet haben. Das Reinigungsmittel sollte auf das Tuch und nicht direkt auf die Touchoberfläche aufgesprüht werden.

Über das Symbol

am Desktop kann der Touch Clean Modus aktiviert werden, der die Touchoberfläche des Displays für eine eingestellte Zeit (mindestens 20 Sekunden) deaktiviert. In dieser Zeit kann das Display gereinigt werden, ohne unbeabsichtigt Aktionen über die Touchoberfläche auszulösen.

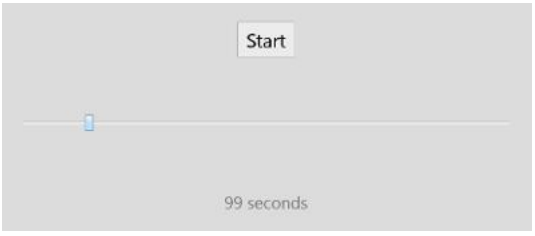


Abb. 13-101: Touch Clean Modus

Nach Ablauf der Zeit wird wieder der Desktop angezeigt.

© KEBA 2021

13.2 Wechseln des Akkus

Falls der Akku trotz vollständiger Aufladung nicht mehr leistungsfähig ist, kann dieser gewechselt werden. Ein neuer Akku kann bei KEBA bestellt werden.

Information

- Die Dichtung des Anschlussschachts muss sauber und unbeschädigt sein und sich an der richtigen Position befinden.
- Es dürfen keine Kabel eingeklemmt werden.

Zum Wechseln gehen Sie wie folgt vor:

1) Ausschalten der Versorgungsspannung.
2) Demontieren des Handbediengeräts.
3) Lösen der 4 Schrauben mittels Schraubendreher (siehe 4.6.2 Akku anstecken).
4) Abnehmen des Anschlussschachtdeckels.
5) Abstecken des Akku-Anschlusskabels im Anschlussschacht.
6) Anstecken des neuen Akku-Anschlusskabels im Anschlussschacht.
7) Schließen des Anschlussschachtdeckels.
8) Festschrauben des Anschlussschachtdeckels mittels Schraubendreher (Drehmoment: 0,8 bis 1,0 Nm).

Der Akku ist gewechselt.

Information

Um der Informationspflicht nachzukommen, werden detaillierte Informationen des Akkus im Produktsicherheits-Datenblatt bereitgestellt. Das Dokument kann auf https://support.keba.com (unter "Verordnungen") heruntergeladen werden.

13.3 Erstellen eines Service Mediums

Ein Service Medium mit dem Programm Bootable Service System (BSS) wird zum Erstellen / Wiederherstellen eines Backups bzw. zum Durchführen eines Updates benötigt.

Um ein Service Medium mit lauffähigem Bootable Service System (BSS) zu erstellen, kann entweder das BSS (z.B. als *.zip Datei) beim KEBA-Support bezogen oder über KeStudio erstellt werden.

Für das Erstellen eines Service Mediums wird folgendes benötigt:

- Leeren USB-Stick mit mind. 32 GB freien Speicherplatz und FAT32 formatiert.

KEBA © KEBA 2021

Erstellen über Archiv-Datei

Zum Erstellen eines Service Mediums über eine Archiv-Datei (z.B. *.zip) muss das von KEBA zur Verfügung gestellte Archiv auf einem Windows-PC extrahiert und in das Verzeichnis `\boot` auf das Wurzelverzeichnis des Service Mediums kopiert werden. Anschließend muss die Datei `prepare.cmd` im Verzeichnis `\boot` ausgeführt werden. Dazu sind Administrator-Rechte notwendig.

Erstellen über KeStudio

Zum Erstellen eines Service Mediums über KeStudio siehe Onlinehilfe.

13.4 Erstellen eines Backups

Für den Backup-Vorgang wird folgendes benötigt:

- Service Medium (USB-Stick) mit mind. 20 GB freiem Speicherplatz

Für weitere Informationen zum Erstellen eines Service Mediums siehe 13.3 Erstellen eines Service Mediums.

Information

Es wird empfohlen, die erstellten Backupdateien auf ein gesichertes EDV-System zu kopieren, da die Datensicherheit auf einem Service Medium über längere Zeit nicht garantiert werden kann.

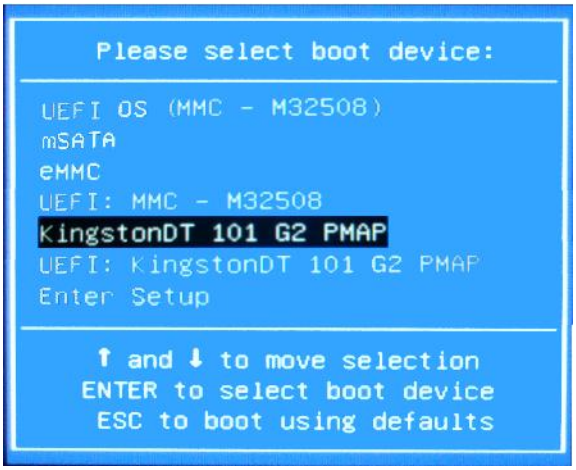
Zum Durchführen des Backups wird zusätzlich zum Service-Medium Folgendes benötigt:

- USB-Hub
- USB-Tastatur

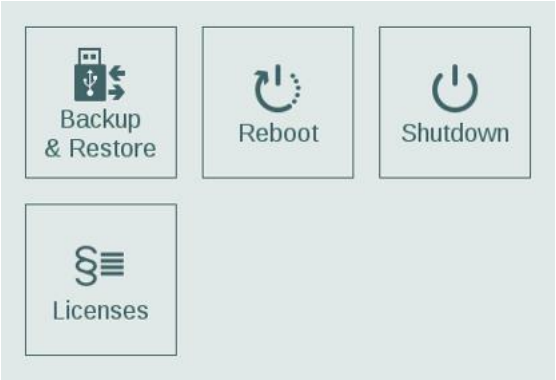
Um das Backup durchzuführen, gehen Sie wie folgt vor:

1) Anstecken des USB-Hubs am KeTop.
2) Anstecken des Service Mediums und der Tastatur am USB-Hub.
3) Durchführen eines Neustarts (Spannungsversorgung trennen und erneut herstellen).
4) Während des Bootvorganges drücken von F7 (auf der USB-Tastatur) beim Erscheinen des Splashscreens, um in das BIOS einzusteigen.
5) Eingabe des BIOS-Passworts 7090. Es dauert ca. 30 Sekunden, bis das BIOS-Bootmenü angezeigt wird.
6) Auswahl des Service Mediums und drücken von Enter.

© KEBA 2021

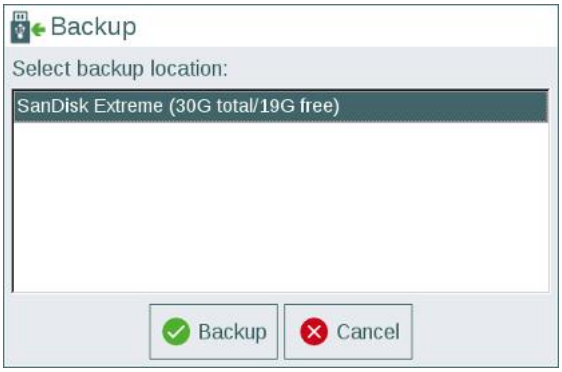


7) Auswählen des Menüpunktes "Backup & Restore" im gestarteten BSS.



8) Wählen von "Backup" in dem angezeigten Menü.

9) Auswahl des Mediums, auf dem das Backup gespeichert werden soll und bestätigen mit "Backup".



10) Bestätigen und Starten des Backups mit der Schaltfläche "OK". Ein Fortschrittsbalken wird angezeigt. Der Vorgang dauert zwischen 15 Minuten und 1 Stunde, abhängig vom verwendeten USB-Stick.

KEBA © KEBA 2021

Information

Das Speichermedium darf nie während des Schreibvorgangs entfernt werden!

11) Nach erfolgreichem Backup-Vorgang bestätigen des Dialogs.

12) Abziehen des USB Hubs.

13) Wählen von "Shutdown" zum Ausschalten oder "Reboot" zum Neustarten des Handbediengeräts im angezeigten Menü.

Das Backup wurde erstellt und auf dem Service Medium im Verzeichnis `\images` gespeichert. Für jedes Backup wird ein Verzeichnis mit Gerätebezeichnung, Datum und Uhrzeit angelegt.

Das Durchführen des Backups unterscheidet sich je nach Prozessor des Gerätes (siehe "Technische Daten").

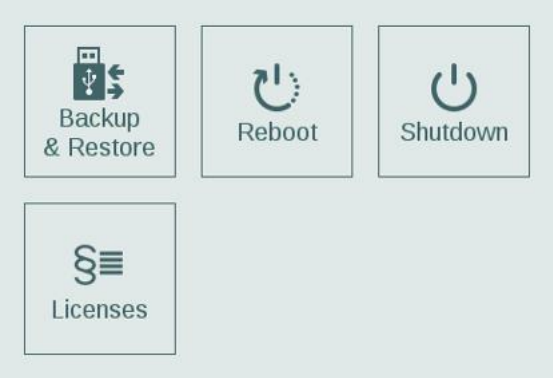
Backup durchführen (für Geräte mit Prozessor "Atom x6211")

Um das Backup durchzuführen, gehen Sie wie folgt vor:

1) Anstecken des vorbereiteten Service Mediums am KeTop.

2) Durchführen eines Neustarts (Spannungsversorgung trennen und erneut herstellen).

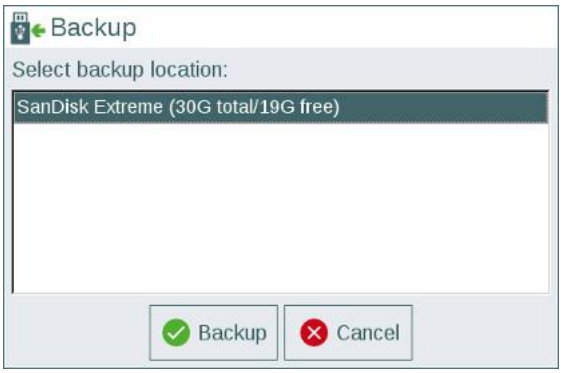
3) Auswählen des Menüpunktes "Backup & Restore" im BSS.



4) Wählen von "Backup" in dem angezeigten Menü.

5) Auswahl des Mediums, auf dem das Backup gespeichert werden soll und bestätigen mit "Backup".

© KEBA 2021



6) Bestätigen und Starten des Backups mit der Schaltfläche "OK". Ein Fortschrittsbalken wird angezeigt. Der Vorgang dauert zwischen 15 Minuten und 1 Stunde, abhängig vom verwendeten USB-Stick.

Information

Das Speichermedium darf nie während des Schreibvorgangs entfernt werden!

7) Nach erfolgreichem Backup-Vorgang bestätigen des Dialogs.
8) Abziehen des Service Mediums.
9) Wählen von "Shutdown" zum Ausschalten oder "Reboot" zum Neustarten des Handbediengeräts im angezeigten Menü.

Das Backup wurde erstellt und auf dem Service Medium im Verzeichnis `\images` gespeichert. Für jedes Backup wird ein Verzeichnis mit Gerätebezeichnung, Datum und Uhrzeit angelegt.

13.5 Wiederherstellen eines Backups / Durchführen eines Updates

Für das Wiederherstellen eines Backups (Restore) bzw. das Durchführen eines Software / Firmware Updates wird folgendes benötigt:

- Service Medium (USB-Stick) mit mind. 20 GB freiem Speicherplatz
- Backup- bzw. Update-Dateien

Für weitere Informationen zum Erstellen eines Service Mediums siehe 13.3 Erstellen eines Service Mediums.

Um ein Backup wiederherzustellen oder ein Update durchzuführen, muss im Wurzelverzeichnis des Service Mediums ein Verzeichnis `\images` angelegt werden. In dieses Verzeichnis müssen die Backup- bzw. Update Dateien kopiert werden.

KEBA © KEBA 2021

Information

Ein Backup darf nur auf dem Gerät wiederhergestellt werden, auf dem es erstellt wurde. Das Klonen von Geräten ist nicht zulässig.

Achtung

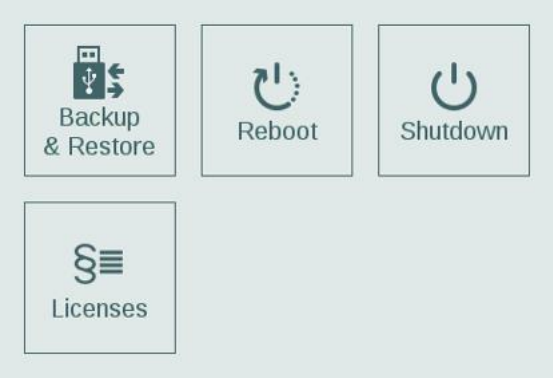
Während eines Vorganges darf das Service Medium nicht gezogen werden. Es muss eine dauerhafte Spannungsversorgung gewährleistet sein (z.B. vollgeladener Akku, Anstecken des Geräts an der Ladestation). Andernfalls kann es zu einer Zerstörung der Firmware auf den Komponenten führen und somit einen weiteren Betrieb unmöglich machen.

Das Wiederherstellen des Backups bzw. Durchführen eines Updates unterscheidet sich je nach Prozessor des Gerätes (siehe "Technische Daten").

Wiederherstellen eines Backups / Durchführen eines Updates (für Geräte mit Prozessor "Atom x6211")

Für diesen Vorgang gehen Sie wie folgt vor:

1) Anstecken des vorbereiteten Service Mediums am KeTop.
2) Durchführen eines Neustarts (Spannungsversorgung trennen und erneut herstellen).
3) Auswählen des Menüpunktes "Backup & Restore" im BSS.



4) Wählen von "Restore" in dem angezeigten Menü.
5) Wählen des gewünschten Service Mediums als Quelle für die Wiederherstellung oder das Update und bestätigen mit der Schaltfläche "Restore".

© KEBA 2021

6) Durch Drücken von "OK" des Bestätigungsdialogs wird der Restore-/ Update-Vorgang gestartet und ein Fortschrittsbalken angezeigt. Der Vorgang dauert etwa 15 - 20 Minuten abhängig vom verwendeten USB-Stick.

Information

Das Speichermedium darf nie während des Schreibvorgangs entfernt werden!

7) Nach erfolgreicher Durchführung Bestätigen des Dialogs.
8) Abziehen des Service Mediums
9) Wählen von "Reboot" zum Neustarten des Handbediengeräts im angezeigten Menü.

Information

Nach dem Neustart führt Windows den Konfigurationsprozess aus. Dies kann mehrere Minuten dauern und endet mit der Aufforderung zur Vergabe eines Windows-Passworts.

*Der Konfigurationsprozess darf **nicht** unterbrochen werden.*

Das Backup wurde wiederhergestellt bzw. das Update durchgeführt.

Für diesen Vorgang wird zusätzlich zum Service-Medium Folgendes benötigt:

- USB-Hub
- USB-Tastatur

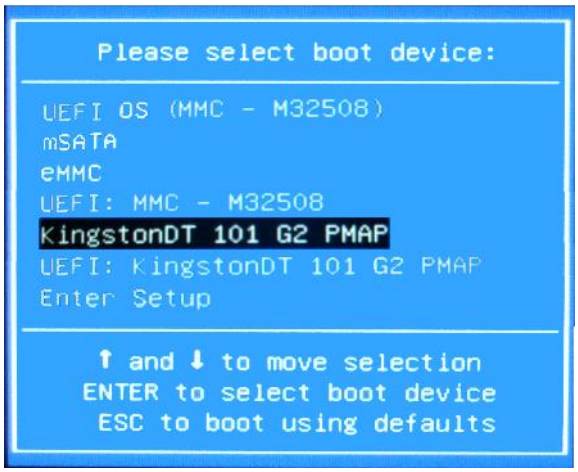
Um den Vorgang durchzuführen, gehen Sie wie folgt vor:

1) Anstecken des USB-Hubs am KeTop.
2) Anstecken des Service Mediums und der Tastatur am USB-Hub.
3) Durchführen eines Neustarts (Spannungsversorgung trennen und erneut herstellen).
4) Während des Bootvorganges drücken von F7 (auf der USB-Tastatur) beim Erscheinen des Splashscreens, um in das BIOS einzusteigen.

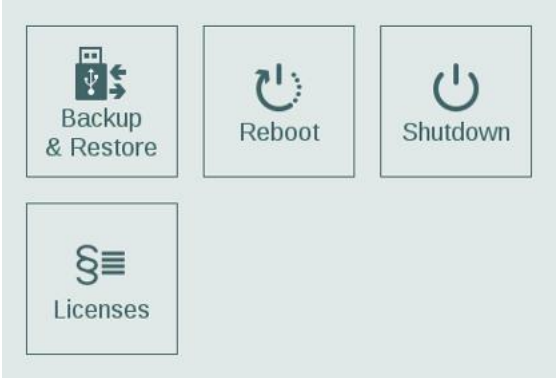
KEBA © KEBA 2021

5) Eingabe des BIOS-Passworts 7090. Es dauert ca. 30 Sekunden, bis das BIOS-Bootmenü angezeigt wird.

6) Auswahl des Service Mediums und drücken von Enter.



7) Auswählen des Menüpunktes "Backup & Restore" im BSS.



8) Wählen von "Restore" in dem angezeigten Menü.

9) Wählen des gewünschten Service Mediums als Quelle für die Wiederherstellung oder das Update und bestätigen mit der Schaltfläche "Restore".

© KEBA 2021

10) Durch Drücken von "OK" des Bestätigungsdialogs wird der Restore-/ Update-Vorgang gestartet und ein Fortschrittsbalken angezeigt. Der Vorgang dauert etwa 15 - 20 Minuten abhängig vom verwendeten USB-Stick.

Information

Das Speichermedium darf nie während des Schreibvorgangs entfernt werden!

11) Nach erfolgreicher Durchführung Bestätigen des Dialogs.

12) Abziehen des USB-Hubs.

13) Wählen von "Reboot" zum Neustarten des Handbediengeräts im angezeigten Menü.

Information

Nach dem Neustart führt Windows den Konfigurationsprozess aus. Dies kann mehrere Minuten dauern und endet mit der Aufforderung zur Vergabe eines Windows-Passworts.

*Der Konfigurationsprozess darf **nicht** unterbrochen werden.*

Das Backup wurde wiederhergestellt bzw. das Update durchgeführt.

Sehen Sie dazu auch

Verbinden mit Basisstation [} 195]

13.6 Wechseln der Speicherkarte

Zum Wechseln der Speicherkarte am Handbediengerät gehen Sie wie folgt vor:

1) Versorgungsspannung abschalten.
2) Öffnen des Anschlussschachts.
3) Alte Speicherkarte bis zum hörbaren Klicken leicht in den Einschubschacht drücken und die losgelöste Speicherkarte entnehmen.
4) Die neue Speicherkarte bis zum Einrasten (hörbares Klicken) leicht in den Einschubschacht drücken, wodurch diese verriegelt wird. Auf korrekte Einsteckrichtung achten!
5) Schließen des Anschlussschachts.

Die Speicherkarte wurde getauscht.

Vorsichtsmaßnahmen beim Umgang mit Flash-Speicher-Medien

Durch falsches Einstecken können Kontaktstifte beschädigt werden.

KEBA © KEBA 2021

Das Speichermedium **nicht gewaltsam** in die Aufnahme einführen. Es ist so konstruiert, dass es nur in einer Richtung in die Aufnahme eingeführt werden kann und es sollte mit ganz geringem Kraftaufwand in die Aufnahme gleiten.

Das Flash-Speicher-Medium:

- von Feuchtigkeit, Hitze und direktem Sonnenlicht fernhalten,
- vor Entladung statischer Elektrizität schützen,
- nicht fallen lassen und nicht biegen,
- nicht entfernen oder das Gerät abschalten, während ein Schreibvorgang darauf aktiv ist.

© KEBA 2021

14 Entsorgung

14.1 Entsorgung der Baugruppe

Achtung

Bitte beachten Sie die Bestimmungen zur Entsorgung von Elektro- und Elektronikgeräten!

Elektro- und Elektronikgeräte inklusive Zubehör sind fachgerecht zu entsorgen. Die Werkstoffe sind gemäß ihrer Kennzeichnung wieder verwertbar. Mit der Wiederverwendung, der stofflichen Verwertung oder anderen Formen der Verwertung von Altgeräten leisten Sie einen wichtigen Beitrag zum Schutz unserer Umwelt.

Das Produkt darf nicht über den Hausmüll entsorgt werden.

14.2 Entsorgung des Akkus

Das Symbol der durchgestrichenen Mülltonne weist darauf hin, dass Akkus nicht über den Hausmüll entsorgt werden dürfen.

Bei der Entsorgung von Akkus sind die nationalen und lokalen Bestimmungen für die fachgerechte Entsorgung zu beachten.Obwohl Akkus eine niedrige Spannung haben, können sie auf starke Wärmezufuhr und mechanische Beschädigungen reagieren. Durch sorgfältige Handhabung und fachgerechte Entsorgung lässt sich das Auftreten von unkontrollierten, gefährlichen Reaktionen jedoch weitgehend verhindern. Zur Verhinderung von Kurzschlüssen und damit einhergehender Erwärmung dürfen Akkus niemals mit leitfähigen Materialien entsorgt werden. Vor dem Entsorgen sind, wenn möglich, die Kontakte mit Klebestreifen zu isolieren.

KEBA © KEBA 2021

VORSICHT!

Personengefährdung durch Brandgefahr oder Verätzung!

- Der Akku darf nur für den bestimmten Gebrauch verwendet werden.
- Der Akku darf weder zerlegt, geöffnet noch zerkleinert werden.
- Der Akku darf nicht kurzgeschlossen werden.
- Ladekabel oder Ladeschale dürfen keine Beschädigungen aufweisen.
- Im Falle eines Auslaufens eines Akkus darf die Flüssigkeit nicht mit der Haut oder den Augen in Berührung kommen. Bei Berührung die betroffene Stelle mit reichlich Wasser abwaschen und einen Arzt aufsuchen.
- Der Akku darf keinen mechanischen Schocks, Druck, Schlägen oder punktuellen Belastungen ausgesetzt werden.
- Der Akku darf weder Feuer noch Hitze ausgesetzt werden.
- Der Akku darf keinem Schmutz oder Feuchtigkeit ausgesetzt werden.
- Den Akku darf nicht im Restmüll entsorgt, sondern muss unter Beachtung der nationalen und lokalen Vorschriften dem ordnungsgemäßen Recycling zugeführt werden. Der Akku darf nur vollständig entleert entsorgt werden. Andernfalls müssen die Kontakte mit Klebestreifen isoliert werden, um einen Kurzsschluss zu vermeiden.
- Der Akku darf nur durch einen von KEBA bezogenen Akku getauscht werden. Bei Verwendung eines anderen Akkus besteht Brand- oder Explosionsgefahr.

© KEBA 2021

Achtung

Ausfall der Akkus durch unsachgemäße Verwendung!

Der Akku muss vor der ersten Verwendung geladen werden.

- Die Lagerung in direkter Sonneneinstrahlung ist zu vermeiden.
- Die Batterie ist an einem kühlen, trockenen und gut belüfteten Ort zu lagern.
- Die Batterie ist in einer staubfreien Umgebung ohne korrosive Gase zu lagern.
- Die Batterie darf nicht länger als 24 Stunden im Ladegerät verbleiben.
- Der Akku muss vor der ersten Verwendung vollständig aufgeladen werden.
- Der Akku darf nur in der Originalverpackung gelagert werden. Behältnisse, in denen Kurzschlüsse mit losen metallischen Gegenständen verursacht werden können, sind zu vermeiden.
- Lagern Sie die Batterie ohne Verpackung nicht in Behältnissen in denen Kurzschlüsse mit losen metallischen Gegenständen verursacht werden können.
- Der Akku darf nicht länger als 1 Monat in entladenem Zustand gelagert werden.

KEBA © KEBA 2021

15 Technische Daten

15.1 Allgemein

Schutzklasse:	III nach EN 61131-2 bzw. EN 50178
Schutzart:	IP65

15.2 Umgebungsbedingungen

Betriebstemperatur:	
• Handbediengerät:	0 °C bis 40 °C
• Basisstation:	0 °C bis 50 °C
Lager- und Transporttemperatur:	
• Handbediengerät mit Akku:	-25 °C bis +50 °C
• Handbediengerät ohne Akku:	-25 °C bis +70 °C
• Basisstation:	-25 °C bis +70 °C
Relative Luftfeuchtigkeit (nicht kondensierend):	5 % bis 95 % (nicht kondensierend)
Vibrationsfestigkeit laut IEC 60068-2-6:	
• Mit 3,5 mm:	5 Hz ≤ f < 8,4 Hz
• Mit 1 g:	8,4 Hz ≤ f < 150 Hz
Schockfestigkeit laut EN 61131-2 bzw. EN 60068-2-27:	15 g / 11 ms
Einsatzhöhe:	Max. 2.000 m Seehöhe

15.3 Sicherheitskennwerte

Handbediengerät allgemein

Gebrauchsdauer:	20 Jahre
Not-Halt:	SIL 3, Kategorie 4, PL e
Zustimmtaster:	SIL 3, Kategorie 4, PL e

WARNUNG!

Um die Kennwerte zu gewährleisten ist das Handbediengerät nach 250.000 Betätigungen des integrierten Not-Halt Schaltelements und/oder 1.000.000 Betätigungen des integrierten Zustimmtasters Schaltelements oder spätestens nach 20 Jahren (Gebrauchsdauer) außer Betrieb zu nehmen.

T15xWL mit Not-Halt (Typ FRVKD_R0)

PFH_D-Wert:	$1{,}05^{-09}$ 1/h
$MTTF_D$[a]-Wert:	356

© KEBA 2021

DC_{avg}-Wert:	98 %
Klassifizierung:	HIGH
$B10_D$-Wert:	250.000
n_{op}-Wert (typisch):	52

T15xWL mit Zustimmtaster (Typ HE6B)

PFH_D-Wert:	$1{,}53^{-09}$ 1/h
$MTTF_D$[a]-Wert:	310
DC_{avg}-Wert:	98 %
Klassifizierung:	HIGH
$B10_D$-Wert:	2.000.000
n_{op}-Wert (typisch):	8.760

T15xWL mit Zustimmtaster (Panik-Kontakt, Typ HE6B)

PFH_D-Wert:	$1{,}03^{-09}$ 1/h
$MTTF_D$[a]-Wert:	358
DC_{avg}-Wert:	98 %
Klassifizierung:	HIGH
$B10_D$-Wert:	1.000.000
n_{op}-Wert (typisch):	52

Basisstation allgemein

Gebrauchsdauer:	20 Jahre
Not-Halt:	SIL 3, Kategorie 4, PL e
Systemreaktionszeit Not-Halt:	19 ms

WARNUNG!

Um die Kennwerte zu gewährleisten ist die Basisstation nach 250.000 Betätigungen des integrierten Not-Halt Schaltelements oder spätestens nach 20 Jahren (Gebrauchsdauer) außer Betrieb zu nehmen.

CB410 / CB42x / CB43x mit Not-Halt (Typ FRVKOO)

PFH_D-Wert:	$1{,}11^{-09}$ 1/h
$MTTF_D$[a]-Wert:	254
DC_{avg}-Wert:	98 %
Klassifizierung:	HIGH
$B10_D$-Wert:	100.000
n_{op}-Wert (typisch):	52

System

Gebrauchsdauer:	20 Jahre
Not-Halt:	SIL 3, Kategorie 4, PL e

KEBA © KEBA 2021

Zustimmtaster:	SIL 3, Kategorie 4, PL e
Systemreaktionszeit (WCDT)*):	430 ms

*) Die Systemreaktionszeit ist die Zeit zwischen Betätigung des Not-Halt bzw. Zustimmtaster bis zum Schalten der Ausgänge auf der Basisstation ("worst-case" Betrachtung). Die Höhe der Systemreaktionszeit wurde von KEBA empirisch ermittelt und gewährleistet ein stabiles System im gewöhnlichen, industriellen Funkumfeld. Typische Reaktionszeiten des Systems liegen im Bereich von 40 - 80 ms. Sollte im Rahmen der allgemeinen Sicherheitsbetrachtung der Bedarf entstehen, die Systemreaktionszeit anzupassen, wenden Sie sich bitte an KEBA.

CB42x PROFIsafe-Kennwerte

DAT (Device Acknowledge Time):	61 ms

MTTF Berechnung

Für die Berechnung der Gesamtsicherheitsfunktion ist der angegebene gesamt PFH_D der Sicherheitselektronik zu verwenden. Der beleuchtete Not-Halt am Handbediengerät und der Not-Halt auf der Basisstation sind zusätzlich zu betrachten. Basis hierfür ist der spezifizierte B_{10D} Wert. Aus diesem muss wie folgt der $MTTF_D$ Wert berechnet werden:

$$MTTF_D = \frac{B_{10D}}{0{,}1 * n_{op}} \qquad n_{op} = \frac{d_{op} * h_{op} * 3600}{t_{Zyklus}} \qquad MTTF_D = \frac{B_{10D} * t_{Zyklus}}{360 * d_{op} * h_{op}}$$

Details zu den Abkürzungen siehe Kapitel 1.7.3 Abkürzungen. Dieser $MTTF_D$ Wert kann nun in einen PFH_D überführt werden (x = Anzahl der Stunden pro Jahr):

$$MTTF_D = \frac{1}{x * PFH_D} = \frac{1}{8760 * PFH_D}$$

Anschließend sind die PFH_D Werte der Gesamtsicherheitsfunktion lt. EN ISO 13849-1 zu addieren:

$PFH_D = PFH_{D\text{-}"Elektronik"} + PFH_{D2\text{-}"Schaltelement"} + ... + PFH_{DN}$

15.3.1 Systemreaktionszeit mit sicherer Feldbusanbindung (bei CB42x und CB43x)

Für die Berechnung der Ansprechzeit der Sicherheitsfunktion, muss von der maximalen Verzögerungszeit des Wireless-Systems im Fehlerfall (WCDT) ausgegangen werden. Zusätzlich ist noch die Watchdog-Zeit des sicheren Feldbusses sowie die Zykluszeit des F-Hosts zu berücksichtigen.

© KEBA 2021

Information

In diesem Handbuch wird nur die Ansprechzeit der Sicherheitsfunktion zwischen Wireless-System und dem F-Host angegeben. Mögliche weitere Sicherheitsmodule (z.B. sichere digitale Ausgangsmodule) werden hier nicht betrachtet.

Zur Berechnung steht folgende Formel zur Verfügung:

OFDT	Worst-case Verzögerungszeit im Fehlerfall (one fault delay time)
WCDT	Worst-case Verzögerungszeit (Worst-case delay time) (Systemreaktionszeit siehe 15.3 Sicherheitskennwerte)
WDTime	Watchdogzeit der sicheren Feldbusverbindung
$Tcy_{F\text{-}Host}$	Zykluszeit des F-Host (F-Host cycle time)

$OFDT = WCDT + WDTime + Tcy_{F\text{-}Host}$

15.4 Mechanische Eigenschaften

Handbediengerät

Konstruktion:	Gehäuse aus PPE/PS
Flammwidrigkeit:	UL94-V0
Falltauglichkeit (2 Fälle nach EN 61131-2):	1 m (auf Industrieboden), danach noch mindestens Schutzart IP54

Basisstation

Konstruktion:	Gehäuse aus ABS-PC

15.5 Batterie / Akku

Batterie – Panasonic BR2032

Herstellername:	Panasonic
Batteriekategorie:	Gerätebatterie
Modellbezeichnung:	BR2032
Chemische Zusammensetzung:	Lithium-Polycarbonmonofluorid-Batterie
Gewicht der Batterie:	8 g
Nennspannung:	3 V
Kapazität:	1000 mAh
Wiederaufladbar:	Nein
Austauschbar:	Nein

Akku - Celltech 169-2001

Herstellername:	Celltech
Batteriekategorie:	Gerätebatterie

KEBA © KEBA 2021

Modellbezeichnung:	169-2001
Chemische Zusammensetzung:	LI-IO
Gewicht der Batterie:	100 g
Nennspannung:	7,2 V
Kapazität:	3450 mAh
Wiederaufladbar:	Ja
Austauschbar:	Ja

15.6 Technische Daten Handbediengerät

15.6.1 Allgemein

Display:	10,1" TFT (16:10) LED-backlight 1.280 x 800 Pixel (WXGA)
Touchscreen:	Projiziert kapazitiv
Tastatur:	Folientastatur mit taktiler Rückmeldung Maximal 30 Tasten 6 Status LEDs

15.6.2 Versorgung

Handbediengerät

Ladespannung:	24 V DC (Nennspannungstoleranzbereich 19,2 V DC bis 29 V DC SELV / PELV nach EN 61010-2-201)
Leistungsaufnahme:	bis 43 W (1,8 A bei 24 V DC)
Anschlussmöglichkeit:	Versorgung über Ladekontakte oder DC-Buchse

Akku

Akkuchemie:	Li-Ionen
Nominalspannung:	7,2 V
Nominalkapazität:	3,5 Ah
Energiegehalt:	25,2 Wh
Lademöglichkeit:	Integriert im Handbediengerät über die Geräte-Versorgung
Typische Betriebszeit:	ca. 1,5 h
Typische Ladezeit für 80 % der Kapazität:	ca. 1,2 h

15.6.3 Rechnerkern

Prozessor:	

© KEBA 2021

• KeTop Txx-xxx-x**P**x-xxx, KeTop Txx-xxx-x**R**x-xxx • KeTop Txx-xxx-x**S**x-xxx, KeTop Txx-xxx-x**T**x-xxx	Atom x6211 Dual Core 1,3 GHz
• KeTop Txx-xxx-x**N**x-xxx, KeTop Txx-xxx-x**f**x-xxx	Celeron N2807 Dual Core 1,58 GHz
Speicher RAM:	
• Atom x6211:	4 GB (DDR4x) 8 GB (DDR4x)
• Celeron N2807:	4 GB (DDR3L)
Speicher FLASH (nur Celeron N2807):	8 GB eMMC
Speicher SSD (Erweiterungsspeicher):	64 GB SSD 256 GB SSD
Betriebssystem:	Windows 10 IoT Enterprise 2016 LTSB oder Windows 10 IoT Enterprise 2021 LTSC

15.6.4 Schnittstellen

Funk-Schnittstelle

Anzahl:	3
WLAN:	WIFI 802.11 a b g n ac
• Frequenzbänder:	2.400 - 2.483,5 MHz / 5.150 - 5.350 MHz / 5.470 - 5.725 MHz
• Sendeleistung:	Max. < 10 dBm
• Verschlüsselung:	WPA2-PSK mit CCMP
Bluetooth:	BT 4.2 BLE
• Frequenzbänder:	2.400 - 2.483,5 MHz
• Sendeleistung:	Max. < 10 dBm
Bedienbereichsüberwachung:	
• Frequenzbänder:	2.400 - 2.483,5 MHz
• Sendeleistung:	Max. < -1,21 dBm

USB-Schnittstelle

Anzahl:	1
Typ:	USB 2.0 (Hi-Speed)
Ausgangsstrom:	Max. 500 mA

RFID Schnittstelle (für Verbindung mit Basisstation)

Anzahl:	1
Reichweite:	Min. 2 cm
Transponder Chip:	I-Code SLI (nach ISO 15693)
Frequenzbänder:	13,553 - 13,567 MHz
Sendeleistung:	Max. < 0,15 A/m

KEBA © KEBA 2021

Micro SD-Schnittstelle

Anzahl:	1

15.6.5 Abmessungen, Gewicht

KeTop T150WL

Höhe (inkl. Not-Halt):	284 mm
Breite:	215 mm
Tiefe:	
● Ohne Griff:	69 mm
● Mit Griff:	76 mm
Gewicht:	Ca. 1.450 g

KeTop T155WL

Höhe (inkl. Not-Halt):	215 mm
Breite:	284 mm
Tiefe:	
● Ohne Griff:	69 mm
● Mit Griff:	76 mm
Gewicht:	Ca. 1.450 g

15.7 Technische Daten Basisstation

15.7.1 Versorgung

Spannungsversorgung:	24 V DC (Nennspannungstoleranzbereich 16 V DC bis 30 V DC SELV / PELV nach EN 61010-2-201)
Einschaltstrom:	9 A (für ca. 2 ms)
Leistungsaufnahme:	14,4 W (600 mA bei 24 V DC)
Max. Unterbrechungsdauer der Versorgungs-spannung:	≤ 10 ms (lt. EN 61131-2)

15.7.2 Schnittstellen

Funk-Schnittstelle

Anzahl:	3
WLAN:	WIFI 802.11 a b g n ac
● Frequenzbänder:	2.400 - 2.483,5 MHz / 5.150 - 5.350 MHz / 5.470 - 5.725 MHz
● Sendeleistung:	Max. < 10 dBm
● Verschlüsselung:	WPA2-PSK mit CCMP
Bluetooth:	BT 4.2 BLE

© KEBA 2021

• Frequenzbänder:	2.400 - 2.483,5 MHz
• Sendeleistung:	Max. < 10 dBm
Bedienbereichsüberwachung:	
• Frequenzbänder:	2.400 - 2.483,5 MHz
• Sendeleistung:	Max. < -1,21 dBm

Ethernet-Schnittstellen

Anzahl:	2
Datenübertragungsrate:	100 Mbit/s

EtherCAT-Schnittstellen

Anzahl:	2
Datenübertragungsrate:	100 Mbit/s

PROFINET-Schnittstellen

Anzahl:	2
Datenübertragungsrate:	100 Mbit/s

"Pairing" / "Remote Pairing" Ausgänge

Anzahl:	2
Nennspannung (Ue):	24 V DC
Strombelastbarkeit:	Max. 100 mA
Vorgegebene Polarität:	Nein
Potentialtrennung:	500 V AC (1 min) zum Rest
Ausgangstestung:	Nein

15.7.3 Klemmleisten

Allgemeine Daten

Anschlussart:	Push-in-Federanschluss
Steckbar:	Ja
Leiterquerschnitt starr/flexibel:	0,2 - 1,5 mm²
Leiterquerschnitt AWG / kcmil:	16 - 24
Leiterquerschnitt flexibel mit Aderendhülse ohne Kunststoffhülse:	0,25 - 1,5 mm²
Leiterquerschnitt flexibel mit Aderendhülse mit Kunststoffhülse:	0,25 - 0,75 mm²
Abisolierlänge:	10 mm
Systemreaktionszeit FRB (typisch):	40 ms

Klemmleiste S1

Anzahl:	1

KEBA © KEBA 2021

Ausführung:	CB41x:11-polig CB42x: 2-polig CB43x: 2-polig
Nennspannung (Ue):	24 V DC
Vorgegebene Polarität:	Ja
Potentialtrennung:	Ja
Ausgangstestung:	Nein

Klemmleiste S2

Anzahl:	1
Nennspannung (Ue):	24 V DC
Strombelastbarkeit:	Max. 700 mA
Stromanforderung:	Min. 1 mA
Vorgegebene Polarität:	Nein
Potentialtrennung:	Ja
Ausgangstestung:	Nein

Klemmleiste Signal

Anzahl:	1
Nennspannung (Ua an 24 V Pin):	24 V DC
Strombelastbarkeit:	Max. 100 mA pro Ausgang (Signalfarbe an der Säule) bzw. 500 mA auf 24 V Pin
Vorgegebene Polarität:	Ja
Potentialtrennung:	Nein
Ausgangstestung:	Nein
Ausgangstyp:	Open Collector Ausgang auf GND

Klemmleiste "Fast Response" Buttons

Anzahl:	14
Nennspannung (Ua):	geschaltete 24 V DC gegen GND auf derselben Klemmleiste
Strombelastbarkeit:	Max. 20 mA pro Ausgang
Vorgegebene Polarität:	Ja
Potentialtrennung:	Nein
Ausgangstestung:	Nein

15.7.4 Zustimmfunktion

Funktion

Ausgangstyp:	Sichere Halbleiterausgänge
Schaltelement:	Zweikreisig elektromechanisch
Nennspannung (Ue):	24 V DC
Nennstrom (Ie):	Max. 250 mA (pro Kreis)

© KEBA 2021

Kurzschluss- und Überlastschutz:	Nein
Potentialtrennung:	500 V AC (1 min) zum Rest
Gebrauchskategorie:	DC13 (nach IEC 60947-5-1)
Verpolungsschutz:	Ja
Ausgangstestung:	Ja (Testimpulsdauer <=2ms)
Umgreiffunktion:	Ja
Ausgangssynchronisierung:	Ja

Schaltelement

Schaltelement:	Zweikreisig elektromechanisch
Betätigungskräfte:	
• Von Schalterstellung 1 auf 2:	3 N typisch
• Von Schalterstellung 2 auf 3:	17 N typisch
B_{10D} Wert (1-2-3-1):	1.000.000

15.7.5 Not-Halt-Funktion

Funktion

Ausgangstyp:	Sichere Relaisausgänge
Schaltelement:	Zweikreisig elektromechanisch
Nennspannung (Ue):	24 V DC
Mindeststrom (Ie):	10 mA (pro Kontakt)
Maximale Strombelastbarkeit:	1.000 mA (pro Kontakt)
Gebrauchskategorie:	DC-13 (nach IEC 60947-5-1)
Ausgangssynchronisierung:	Ja
Potentialtrennung:	500 V AC (1 min) zum Rest

Schaltelement

Schaltelement:	Zweikreisig elektromechanisch, Drehentriegelung
B_{10D} Wert:	250 000

Beleuchteter Not-Halt

Beleuchtungstyp:	LED Beleuchtung
Leuchtstärke:	Typ 11700 mcd
Lebensdauer:	Lebensdauer 80.000 - 100.000 h

15.7.6 Abmessungen, Gewicht

CB41x

Höhe:	162 mm
Breite:	221 mm
Tiefe:	70 mm (ohne Not-Halt)

KEBA © KEBA 2021

Gewicht:	Ca. 760 g

CB42x

Höhe:	167 mm
Breite:	223 mm
Tiefe:	95 mm (ohne Not-Halt)
Gewicht:	Ca. 600 g

CB43x

Höhe:	167 mm
Breite:	223 mm
Tiefe:	95 mm (ohne Not-Halt)
Gewicht:	Ca. 600 g

© KEBA 2021

16 Optionale Bedienelemente

Dieses Kapitel beschreibt die verschiedenen Optionsmöglichkeiten, mit denen die Geräte erhältlich sind. Die Optionselemente sind durch den Einbauplatz begrenzt und können sich dadurch gegenseitig ausschließen.

16.1 Drehschalter mit 16 Positionen

Das T15xWL kann mit einem Drehschalter (16 Stellungen, 4 Bit Graycode) ausgestattet sein, der standardmäßig per Software (über HWAPI oder Verbindungsprotokoll) ausgewertet wird.

16.2 Schlüsselschalter

Das T15xWL und die Basisstation können mit einem Schlüsselschalter ausgestattet werden.

Am Handbediengerät kann der Schlüsselschalter per Software (über HWAPI oder Verbindungsprotokoll) ausgewertet werden. Auf der Basisstation ist der Schlüsselschalter direkt verdrahtet und nicht über die Software auswertbar. Der Schlüsselschalter wird nicht von der Sicherheitselektronik ausgewertet und ist daher nicht Teil der Baumusterprüfung.

WARNUNG!

Bei Auswertung eines Schaltelements über die Software kann es durch einen Fehler zu einer falschen Bewertung des Schaltzustandes kommen. Ist die Stellung des Schlüsselschalter sicherheitsrelevant, dann muss dieses elektromechanische Schaltelement direkt (ohne elektronische Auswertung auf KeTop Ebene) in die Sicherheitslogik verdrahtet werden.

Achtung

Die Sicherheitslogik muss die Stellung des Schlüsselschalters auf Exklusivität prüfen, um gleichzeitig mehrfach selektierte Betriebsarten zu erkennen.

Der Schlüsselschalter ist in einer Version mit 3 Stellungen oder mit 2 Stellungen erhältlich.

Abhängig von der Variante des bestückten Schlüsselschalters besitzt dieser eine oder mehrere Abzugspositionen für den Schlüssel.

16.3 Leuchtdrucktaster

Das T15xWL und die Basisstation können mit einem Leuchtdrucktaster ausgestattet werden.

KEBA © KEBA 2021

Am Handbediengerät kann der Leuchtdrucktaster per Software (über HWAPI oder Verbindungsprotokoll) ausgewertet und gesteuert werden. Auf der Basisstation ist der Leuchtdrucktaster direkt verdrahtet und nicht über die Software auswertbar.

Der Leuchtdrucktaster ist mit Impuls- oder Rastfunktion erhältlich.

WARNUNG!

Bei Auswertung eines Schaltelements über die Software kann es durch einen Fehler zu einer falschen Bewertung des Schaltzustandes kommen. Wird das Schaltelements sicherheitsgerichtet verwendet, dann muss dieses elektromechanische Schaltelement direkt (ohne elektronische Auswertung auf KeTop Ebene) in die Sicherheitslogik verdrahtet werden.

16.4 Handrad

Das T15xWL kann mit einem Handrad ausgestattet werden. Die Handrad-Impulse werden im Prozessor ausgewertet und können per Software (über HWAPI oder Verbindungsprotokoll) ausgelesen werden.

Pro Umdrehung werden 50 Impulse gezählt. Eine Drehung des Handrades im Uhrzeigersinn inkrementiert, eine Drehung gegen den Uhrzeigersinn dekrementiert den Zählerstand 0 bis 65.535 (16 Bit Wert).

Wesentliche Merkmale:

- 50 Rastungen / Umdrehung
- 1 Impuls / Rastung

Information

Sollte das KeTop zu Boden fallen, überprüfen Sie den mechanischen Sitz des Drehknopfs. Der Drehknopf kann durch mittiges Andrücken von oben gegebenenfalls wieder eingerastet werden.

16.5 Digitaler Joystick

Das Handbediengerät kann mit einem digitalen Joystick ausgestattet werden. Am Handbediengerät wird der digitale Joystick per Software (über HWApi oder Verbindungsprotokoll) ausgewertet und gesteuert. Auf der Basisstation ist der Joystick direkt verdrahtet und kann deshalb nicht über die Software ausgewertet werden.

Der digitale Joystick kann entlang von 2 Achsen in 4 Richtungen bewegt werden. Die Auslenkung des Joysticks wird mit elektrischen Schließerkontakten erkannt und durch logische Verknüpfungen der 4 Bit verarbeitet.

Wesentliche Merkmale:

- 2 Richtungen / Achse

© KEBA 2021

- 1 Bit / Auslenkung

16.6 Kamera

Das T15xWL kann auf der Rückseite mit einer Kamera ausgestattet werden.

Technische Daten

Video Formate:	YUY2 / MJPEG
USB:	2.0
Bild Auflösung:	5 Megapixel 320 x 240 (min) / 640 x 480 (Standard) / 2592 x 1944 (max)

KEBA © KEBA 2021

17 Zubehör

17.1 KeTop CS 15x Ladestation

Die Ladestation dient als Wandhalterung und zum Aufladen des Gerätes und kann unter folgender Nummer bestellt werden:

Bestellnummer	Gerät
111903	KeTop CS15x

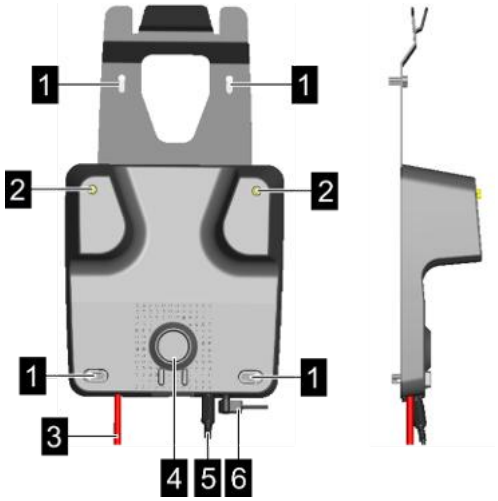


Abb. 17-102: Ladestation

1 ... Bohrloch	2 ... Ladekontakt
3 ... 24 V Stromversorgung über Netzteil Externe Spannungsversorgung	4 ... Magnethalterung für den Zusatz-Akku
5 ... Stecker für 24 V Stromversorgung des Zusatz-Akkus	6 ... 24 V Stromversorgung über direkten Anschluss (Stecker)

Information

Das Handbediengerät kann von der Ladestation nur bei Umgebungstemperaturen unter 40 °C aufgeladen werden.

Stromversorgung über Netzteil

Die Ladestation kann über ein handelsübliches Netzteil mit Strom versorgt werden. Dazu befindet sich eine DC-Buchse 5.5/2.1 passend für einen DC-Hohlstecker 5.5/2.1 an der Ladestation.

© KEBA 2021

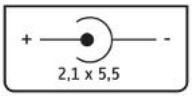


Abb. 17-103: Buchsen Symbol

Stromversorgung über direkten Anschluss

Die Ladestation kann über eine direkte Verdrahtung mit Strom versorgt werden. Dazu muss die Ladestation geöffnet werden.

Abb. 17-104: Stecker

1 ... 24 V (plus)	2 ... GND (minus)

Information

Ein Betrieb der Ladestation ist nur mit korrekt geschlossenem Gehäuse zulässig.

WARNUNG!

Personengefährdung durch elektrischen Schlag!

- Versorgen Sie die Ladestation ausschließlich aus Spannungsquellen, welche Schutzkleinspannung aufweisen (z.B. SELV oder PELV nach EN 61010-2-201).
- Durch das Anschließen einer SELV Spannungsquelle kann diese, bedingt durch die Bauart, zu einer PELV Spannungsquelle werden.
- Schließen Sie an Anschlüsse, Klemmen oder Schnittstellen bis 50 V Nennspannung nur Spannungen und Stromkreise an, welche eine sichere Trennung zu gefährlichen Spannungen haben (z.B. durch ausreichende Isolierung und Spannungsfestigkeit).

KEBA © KEBA 2021

VORSICHT!

Brandgefahr bei Bauteilausfall!

Sorgen Sie bei der Versorgung der Ladestation für eine angemessene Absicherung der 24 V DC Stromversorgung des Gerätes! Es muss dazu eine UL 248 zugelassene Sicherung mit max. 3,15 A verwendet werden.

Laden Sie das Handbediengerät nur mit den seitens KEBA empfohlenen Ladegeräten und mit den vorgesehenen Lademitteln (Ladestation und Netzteil).

17.2 Netzteil

Das Netzteil dient zum Aufladen des Gerätes. Es kann direkt am Handbediengerät oder an der Ladestation angeschlossen werden und kann unter folgender Nummer bestellt werden:

Information

Dieses Netzteil ist ein optionales Zubehörteil, das ausschließlich zur Inbetriebnahme des Wireless Handbediengerätes in Büro bzw. Laborumgebungen bestimmt ist.

Bestellnummer	Bezeichnung
128939	KeTop 24VDC Versorgungsset

Information

Das Netzteil ist nicht für Industrieumgebung geeignet und darf daher nur im Wohnbereich (z.B. Büro) verwendet werden. Da das KeTop im Wohnbereich Funkstörungen verursachen kann, nur im ausgeschalteten Zustand laden.

17.3 Akku

Der interne Akku des Handbediengeräts wird im Handbediengeräts über die Ladestation aufgeladen und kann unter folgender Nummer nachbestellt werden:

Bestellnummer	Gerät
120048	KeTop T150WL Akku V1 (nur Celeron N2807)
120049	KeTop T155WL Akku V1 (nur Celeron N2807)
140626	KeTop T150WL Akku V2 (nur Atom x6211)
140627	KeTop T155WL Akku V2 (nur Atom x6211)
140915	KeTop T150WL Akku V2 (nur Celeron N2807)

© KEBA 2021

Bestellnummer	Gerät
140916	KeTop T155WL Akku V2 (nur Celeron N2807)

Sehen Sie dazu auch

Ruhezustand konfigurieren [› 170]

17.3.1 Akku Celeron N2807

Typenschild

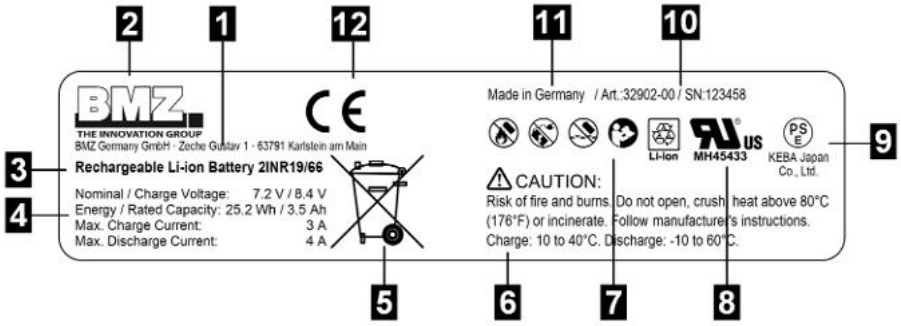


Abb. 17-105: Typenschild

1 ... Herstelleradresse	2 ... Hersteller
3 ... Produktbezeichnung	4 ... Technische Daten
5 ... Entsorgungshinweis	6 ... Warnhinweis
7 ... Warnsymbole	8 ... UR-Prüfzeichen
9 ... PSE-Kennzeichnung	10 ... Artikel- und Seriennummer
11 ... Herstellungsland	12 ... CE-Konformitätskennzeichnung

Akkulaufzeit

Die Akkulaufzeit ist abhängig von der Konfiguration des Handbediengeräts (siehe 8.7 Ruhezustand konfigurieren).

Information

Fällt die Akku-Kapazität auf 25 %, wird eine Warnung ausgegeben. Ab ≤15 % geht das Handbediengerät in den Ruhezustand.

Lagerung und Transport

Im Auslieferzustand ist der Akku abgesteckt und zu 30 % geladen. Dies entspricht dem optimalen Lager- und Transportzustand. Um diesen Zustand zu erhalten, muss der Akku alle 3 Monate am Handbediengerät angesteckt, auf 30 % aufgeladen und wieder abgesteckt werden.

KEBA © KEBA 2021

Vor Inbetriebnahme des Handbediengeräts ist der Akku vollständig aufzuladen.

17.3.1.1 Technische Daten

Umgebungsbedingungen

Betriebstemperatur:	0 °C bis 40 °C
Lager- und Transporttemperatur:	-25 °C bis +50 °C (ideal: 20 °C)
Ladetemperatur:	10 °C bis 40 °C
Relative Luftfeuchtigkeit (nicht kondensierend):	5 % bis 95 % (ideal: 40 °C)
Einsatzhöhe:	Max. 2000 m Seehöhe

17.3.2 Akku Atom x6211

Typenschild

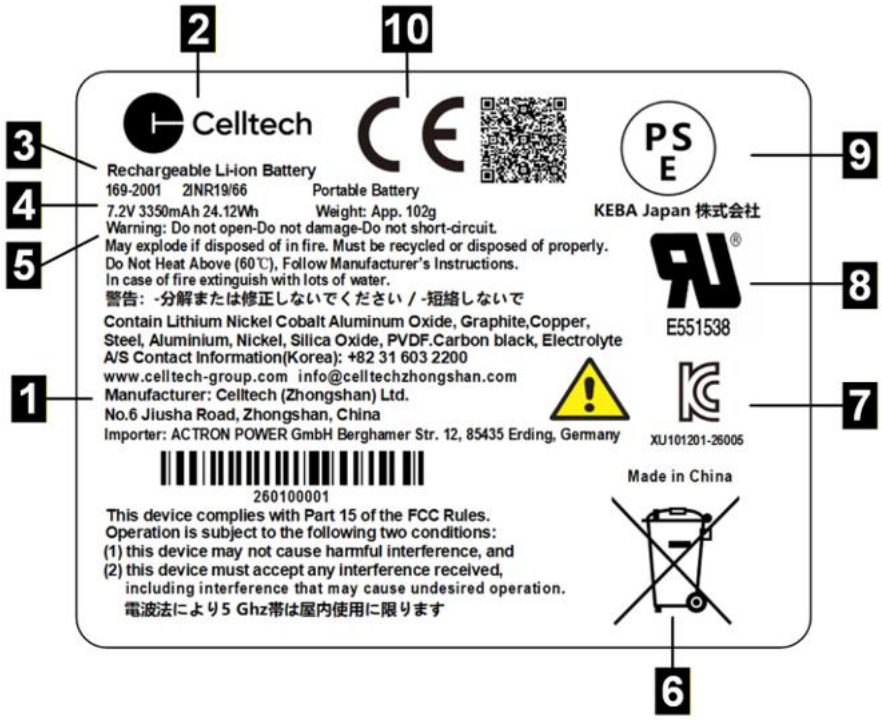


Abb. 17-106: Typenschild

1 ... Herstelleradresse	2 ... Hersteller
3 ... Produktbezeichnung	4 ... Technische Daten
5 ... Warnhinweis	6 ... Entsorgungshinweis
7 ... KC-Kennzeichnung	8 ... UR-Prüfzeichen
9 ... PSE-Kennzeichnung	10 ... CE-Konformitätskennzeichnung

© KEBA 2021

Akkulaufzeit

Die Akkulaufzeit ist abhängig von der Konfiguration des Handbediengeräts (siehe 8.7 Ruhezustand konfigurieren).

Information

Fällt die Akku-Kapazität auf 25 %, wird eine Warnung ausgegeben. Ab ≤15 % geht das Handbediengerät in den Ruhezustand.

Lagerung und Transport

Im Auslieferzustand ist der Akku abgesteckt und zu 30 % geladen. Dies entspricht dem optimalen Lager- und Transportzustand. Um diesen Zustand zu erhalten, muss der Akku alle 3 Monate am Handbediengerät angesteckt, auf 30 % aufgeladen und wieder abgesteckt werden.

Vor Inbetriebnahme des Handbediengeräts ist der Akku vollständig aufzuladen.

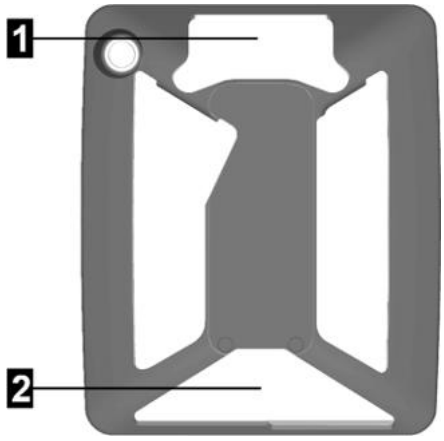
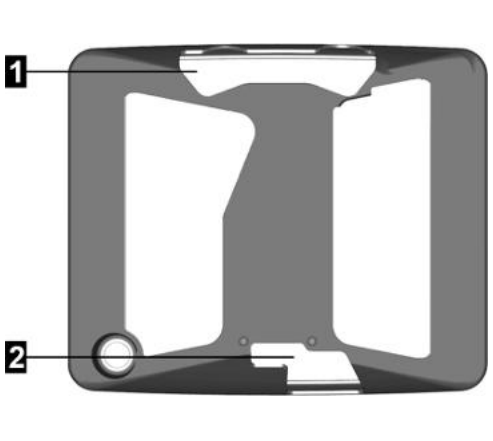
17.3.2.1 Technische Daten

Umgebungsbedingungen

Betriebstemperatur:	-40 °C – 60 °C (Entladen)
Lager- und Transporttemperatur:	-10 °C – 26 °C (1 Jahr)
Ladetemperatur:	0 – 60 °C
Relative Luftfeuchtigkeit (nicht kondensierend):	35 – 85 % (relative Luftfeuchte)
Einsatzhöhe:	Max. 2000 m

17.4 Schutzhülle / Trageset

Die Schutzhülle dient als zusätzlicher Schutz des Handbediengerätes vor Stößen oder Schlägen und ist in folgenden Varianten erhältlich:

Schutzhülle Hochformat	Schutzhülle Querformat
	

KEBA © KEBA 2021

1	Griffausnehmung	2	Kabelausnehmung

Die Schutzhülle kann bei Firma KEBA angefragt und bestellt werden:

Bezeichnung	Bestellnummer
Schutzhülle Hochformat (KeTop T150x)	125248
Schutzhülle Querformat (KeTop T155x)	122868

Trageset

Da Trageset besteht aus der Schutzhülle und einem Tragegurt. Das Trageset dient der ergonomischen Entlastung und erhöhten Bewegungsfreiheit. Zusätzlich wird die Sicherheit und Effizienz im Umgang mit dem Handbediengerät erhöht.

WARNUNG!

Personengefährdung durch Strangulation oder Absturz!

Unsachgemäße Verwendung des Tragesets als Hebezeug für Personen kann zu lebensgefährlichen Verletzungen oder Tod führen. Bewegte Teile im Trageset können zu Verfangen und Strangulation führen.

- Trageset niemals zum Heben oder Sichern von Personen verwenden.
- Beim Umgang mit dem Trageset auf bewegte Teile achten und diese von Körperteilen fernhalten.

WARNUNG!

Gesundheitsgefährdung durch falsche körperliche Belastung!

Einseitige Belastung durch zusätzliche befestigte Zubehör-Teile kann zu Rückenschmerzen sowie weiteren Muskel- und Gelenkverletzungen führen. Die Befestigung nicht zugelassener zusätzlicher Teile am Trageset kann die Sicherheit beeinträchtigen und Verletzungen verursachen.

- Bei Verwendung von Zubehör-Teilen wie Zusatz-Akku eine einseitige Belastung vermeiden.
- Keine weiteren zusätzlichen Teile am Trageset befestigen, die nicht ausdrücklich erlaubt sind.

© KEBA 2021

WARNUNG!

Personengefährdung durch heiße Oberfläche oder Brandgefahr!

Erhitzte Ladepunkte können Verbrennungen verursachen oder ein Feuer im Trageset auslösen, wenn die Ladekontakte nicht korrekt verbunden sind.

- Sicherstellen, dass die Ladekontakte der Ladeschale nicht von einem Gurt des Tragesets überdeckt werden.
- Ladekontakte des Handbediengeräts und der Ladeschale müssen sich flächig berühren, um Überhitzung und Brandgefahr zu vermeiden.

VORSICHT!

Stolpergefahr und Behinderung von Verkehrswegen!

Unsachgemäß abgestellte oder platzierte Handbediengeräte und Tragesets können zu Stolperunfällen und Behinderungen führen, was leichte bis mäßige Verletzungen verursachen kann.

- Handbediengerät inklusive Trageset nur an der Wandhalterung oder Ladeschale anbringen.
- Trageset bei Nichtgebrauch außerhalb von Verkehrs- und Gefahrenbereichen sicher verstauen.

Das Trageset kann bei Firma KEBA angefragt und bestellt werden.

Bezeichnung	Bestellnummer
Trageset mit Bumber Hochformat (KeTop T150)	136171
Trageset mit Bumber Querformat (KeTop T155)	136160

17.4.1 Anbringen der Schutzhülle

Achtung

Unsachgemäße Handhabung kann zur Beschädigung des Handbediengeräts führen.

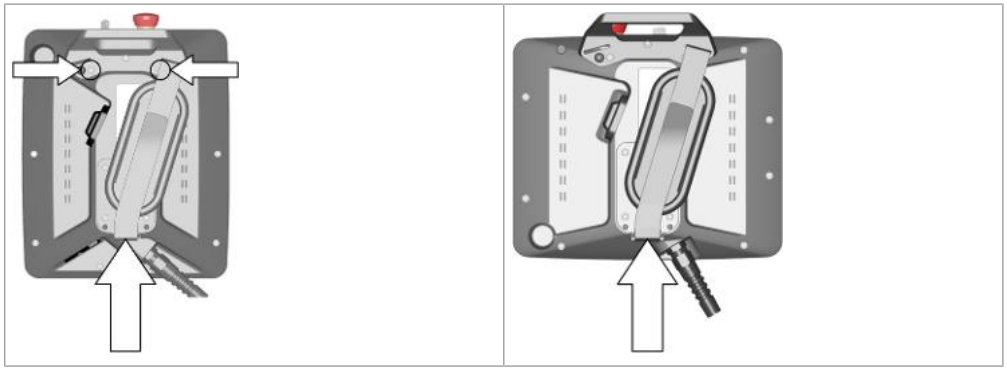
- Vor Montage-, Installations- und Instandhaltungsmaßnahmen die Versorgungsspannung ausschalten und eventuelle Schnittstellenkabel abstecken.
- Auf eine saubere, ebene und stabile Montagefläche achten. Die Fläche sollte frei von Staub und Fremdkörpern sein.
- Verwenden einer Unterlage, um die Glasfront vor Kratzern zu schützen.

Zum Anbringen der Schutzhülle gehen Sie wie folgt vor:

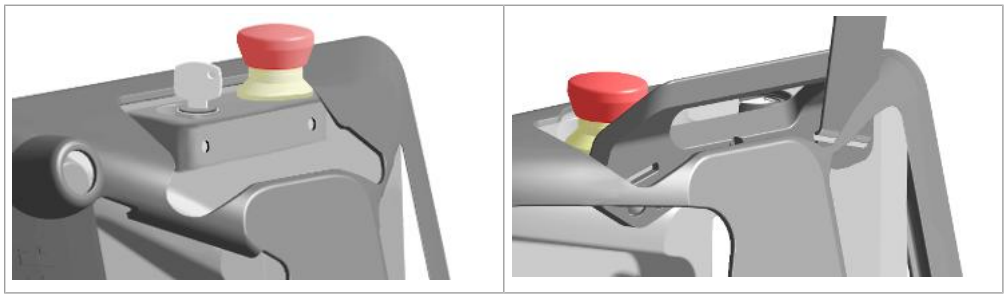
1) Ausschalten der Versorgungsspannung.
2) Falls vorhanden: Abstecken des Anschlusskabels.

KEBA © KEBA 2021

3) Lösen der Handschlaufe am unteren Ende und entfernen des Griffes mit einem Schraubendreher (Torx10).



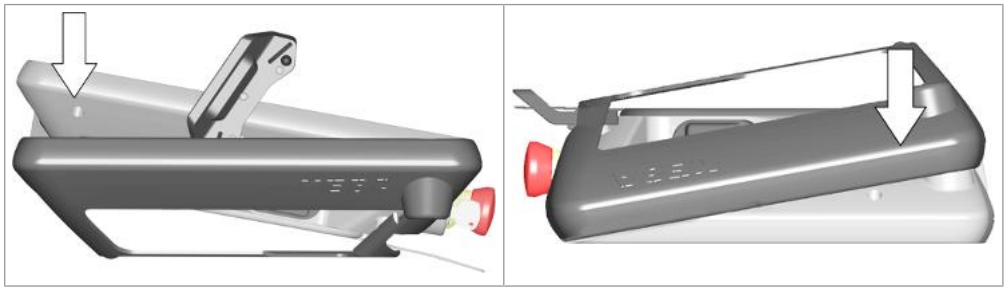
4) Einhängen der Schutzhülle am Not-Halt Schalter über die Griffausnehmung.



5) Falls vorhanden: Durchziehen des Anschlusskabels durch die Kabelausnehmung der Schutzhülle.

6) Stülpen der Schutzhülle über die oberen Ecken.

7) Stülpen der Schutzhülle über die unteren Ecken. Der abmontierte Griff kann als Montagehilfe verwendet werden.



8) Anschrauben des Griffes und montieren der Handschlaufe am unteren Ende des Geräts.

Die Schutzhülle ist am Handbediengerät angebracht.

© KEBA 2021

17.4.2 Reinigung

Achtung

Sachschaden durch unsachgemäße Reinigung oder Trocknung!

Unsachgemäße Reinigung oder Trocknung können das Trageset beschädigen.

Schutzhülle und Tragegurt ausschließlich gemäß den hier angegebenen Anweisungen reinigen und trocknen

Um Schutzhülle und Tragegurt zu reinigen, gehen Sie wie folgt vor:

1) Handbediengerät aus der Schutzhülle entfernen.
2) Reinigung der Schutzhülle mit einer weichen Bürste (trocken oder feucht). Dabei darauf achten, dass keine Etiketten beschädigt oder unlesbar gemacht werden.
3) Händische Reinigung des Tragegurts: Gurtbänder und Seile mit lauwarmen Wasser oder milder lauwarmer Seifenlauge (max. 40 °C) reinigen. Keine Chemikalien verwenden.
4) Abspülen mit klarem lauwarmen Wasser.
5) Trocknen lassen an einem luftigen, trockenen und schattigem Ort. Schutzhülle und Tragegurt nicht unnötiger UV-Strahlung aussetzen.

17.4.3 Lagerung und Transport

Achtung

Sachschaden durch unsachgemäße Lagerung oder unsachgemäßen Transport!

Unsachgemäße Lagerung oder unsachgemäßer Transport können das Trageset beschädigen.

Schutzhülle und Trageset ausschließlich gemäß den hier angegebenen Anweisungen lagern und transportieren.

Schutzhülle und Trageset stets vor UV-Strahlung und Hitze schützen und bei Lagerung und Transport auf ausreichende Belüftung achten. Luftdichte Behälter vermeiden. Es wird empfohlen, einen UV-beständigen Materialsack zu verwenden.

17.5 Griff und Handschlaufe

Am T15xWL kann ein Griff mit oder ohne Handschlaufe montiert werden. Der Griff wird mit 3 Torx Schrauben (Größe 10) befestigt. Die Handschlaufe kann nur bei montiertem Griff verwendet werden.

KEBA © KEBA 2021

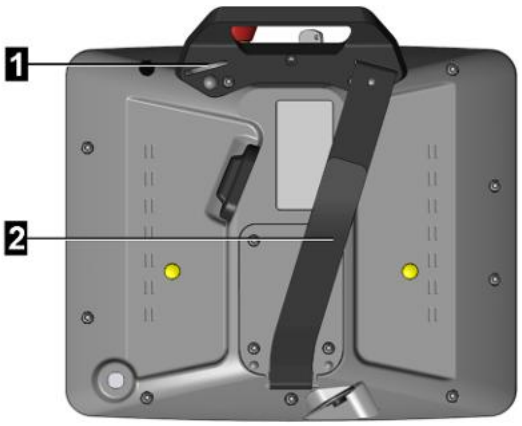


Abb. 17-107: T15xWL mit Griff und Handschlaufe

1 ... Griff	2 ... Handschlaufe

17.5.1 Montage

In diesem Kapitel wird die Montage des Griffs und der Handschlaufe beschrieben. Dazu wird folgendes Set benötigt:

Bezeichnung	Beschreibung	Bestell-Nr.
Griff und Handschlaufe T15x	Montageset für Griff und Handschlaufe für KeTop T150 und KeTop T155	106420

Achtung

- Unsachgemäße Handhabung kann zur Beschädigung des Handbediengeräts führen. Schalten Sie vor Montage-, Installations- und Instandhaltungsarbeiten die Versorgungsspannung aus.
- Achten Sie auf eine saubere, ebene und stabile Montagefläche. Die Fläche sollte frei von Staub und Fremdkörpern sein.
- Verwenden Sie eine Unterlage, um die Glasfront vor Kratzern zu schützen.
- Die Installation und Inbetriebnahme des Produkts darf nur von qualifiziertem Fachpersonal vorgenommen werden.

Folgendes Werkzeug wird benötigt:

- Torx Schraubendreher Größe 10

Um den Griff und die Handschlaufe zu montieren, gehen Sie wie folgt vor:

1) Ausschalten der Versorgungsspannung.
2) Demontieren des Handbediengeräts.
3) Ablegen des Handbediengeräts auf der Montagefläche mit dem Touchscreen nach unten.

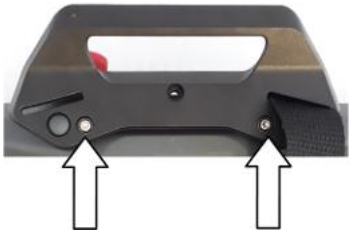
© KEBA 2021

4) Durchfädeln des dünnen Endes der Handschlaufe (1) durch den gewünschten Schlitz am Griff (2). Der Klettverschluss muss dabei nach oben zeigen.

5) Durchziehen der gesamten Handschlaufe von hinten nach vorne bis zum breiten Ende.

6) Anbringen der Polsterung (optional). Der Klettverschluss muss dabei nach oben zeigen (1).

7) Festschrauben des Griffs mittels Schraubendreher (Drehmoment: 0,8 - 1,0 Nm) am oberen Ende des Handbediengeräts.

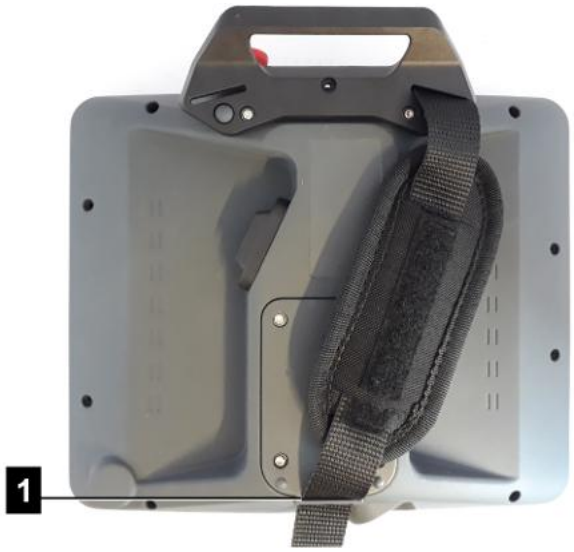


8) Durchfädeln der Handschlaufe durch den Schlitz am unteren Ende des Handbediengeräts (1).

Information

Die Handschlaufe beim Durchfädeln nicht verdrehen.

KEBA © KEBA 2021



9) Durchziehen der gesamten Handschlaufe.

10) Festmachen der Klettverschlüsse aneinander.

Griff und Handschlaufe sind nun fertig montiert und können verwendet werden.

17.6 Zusatz-Akku

Der Zusatz-Akku ("Battery-Pack") kann verwendet werden, um die Laufzeit des Handbediengeräts zu verlängern. Der Zusatz-Akku darf nur mit dem Handbediengerät betrieben werden. Der Zusatz-Akku wird an der Ladestation aufgeladen.

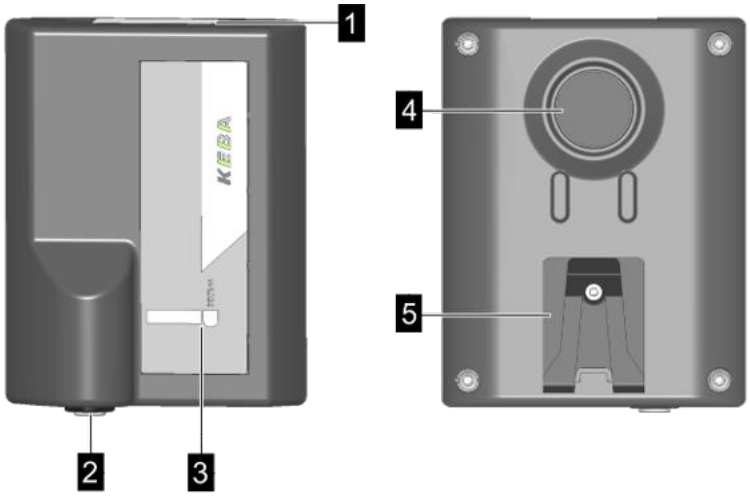


Abb. 17-108: Zusatz-Akku

1 ... Typenschild	2 ... Buchse für 24 V Stromversorgung der Ladestation
3 ... Ladezustands-Anzeige mit Button	4 ... Magnethalterung für Ladestation

© KEBA 2021

5 ... Gürtelhalter (optional)	

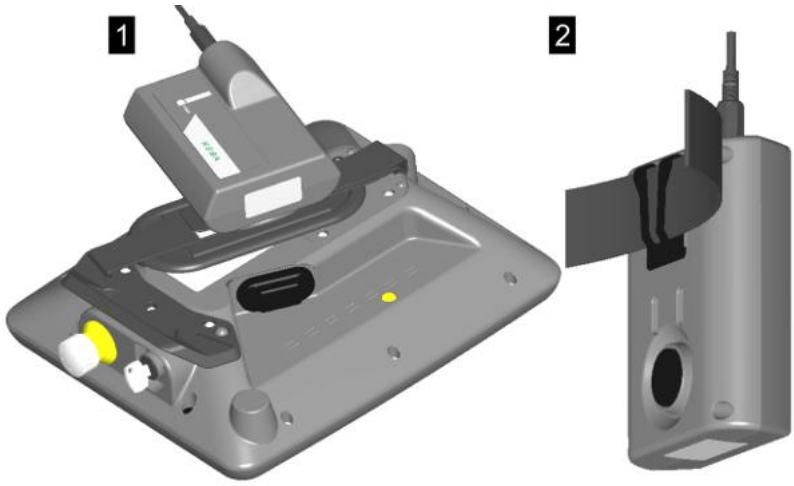


Abb. 17-109: Befestigung des Zusatz-Akkus

1 ... An der Handschlaufe des Handbediengeräts	2 ... Am Gürtel

Der Zusatz-Akku wird am Handbediengerät angesteckt und kann entweder an der Handschlaufe des Geräts oder am Gürtel mittels Gürtelhalter befestigt werden. Der Gürtelhalter wird mit der beiliegenden Schraube (Schraubenkopf Torx 8) an die vorgesehene Stelle geschraubt. Die Schraube mit 0,55 Nm Drehmoment vollständig eindrehen.

Der Zusatz-Akku und das optionale Zubehör können unter folgender Nummer bestellt werden:

Bestellnummer	Bezeichnung	Lieferumfang
131539	KeTop BP15xWL Set	• Akku • Schachtel • Kabel (kurz) • Handschlaufenhalter
133130	Gerätehalter für KeTop BP15xWL	• Kabel (kurz) • Handschlaufenhalter
133131	Gürtelhalter für KeTop BP15xWL	• Kabel (lang) • Gürtelhalter
133179	KeTop BP15xWL	• Akku (ohne Zubehör)

KEBA © KEBA 2021

Typenschild

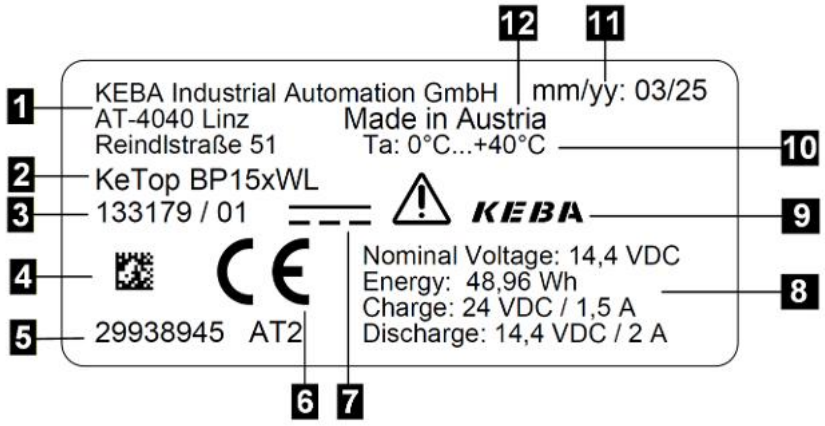


Abb. 17-110: Typenschild

1 ... Herstelleradresse	2 ... Produktbezeichnung
3 ... Material- / Revisionsnummer	4 ... Datamatrix Code
5 ... Seriennummer	6 ... CE-Konformitätskennzeichnung
7 ... Kennzeichnung zur getrennten Entsorgung	8 ... Technische Daten
9 ... Hersteller	10 ... Umgebungstemperatur
11 ... Produktionsdatum	12 ... Herstellungsland

Akkulaufzeit

Durch Drücken des Buttons "PRESS" wird der Ladezustand mit vier LEDs bei der Ladezustands-Anzeige angezeigt:

LED-Muster	Ladezustand
1 LED blinkt	< 10%
1 LED leuchtet	10 % - 25%
2 LEDs leuchten	26 % - 50%
3 LEDs leuchten	51 % - 75%
4 LEDs leuchten	76 % - 100%

Die Lebensdauer des Zusatz-Akku ist abhängig von den Umgebungsbedingungen und der Art der Anwendung. In der Regel sind bis zu 800 Ladezyklen möglich, ohne dass die Kapazität merklich abnimmt.

Lagerung und Transport

Der Zusatz-Akku befindet sich im Auslieferungszustand im Transportmodus. Im Transportmodus kann der Akku längere Zeit ohne Kapazitätsverlust gelagert werden.

© KEBA 2021

Information

Im Transportmodus funktioniert die Ladezustands-Anzeige nicht.

Der Transportmodus wird mit dem ersten Aufladen beendet. Nach dem ersten Aufladen muss der Akku alle 12 Monate aufgeladen werden. Den Zusatz-Akku nach dem ersten Aufladen mit einem Ladezustand von 40 - 60 % lagern.

Entsorgung

Der Zusatz-Akku darf nicht über den Hausmüll entsorgt werden.

Beachten Sie die Hinweise zur fachgerechten Entsorgung (siehe Kapitel 14.2 Entsorgung des Akkus).

Sehen Sie dazu auch

Technische Daten [} 247]

17.6.1 Zusatz-Akku verwenden

Information

Vor der ersten Verwendung muss der Zusatz-Akku vollständig aufgeladen werden.

Um den Zusatz-Akku zu verwenden, gehen Sie wie folgt vor:

1) Das Ladekabel an die Buchse für 24 V Stromversorgung am Zusatz-Akku anschließen.
2) Das andere Ende des Ladekabels an die Buchse für die externe Spannungsversorgung am Handbediengerät anschließen.
3) Den Zusatz-Akku, je nach Ausführung, an der Handschlaufe des Geräts oder am Gürtel anbringen.

Der Zusatz-Akku wird verwendet.

17.6.2 Zusatz-Akku laden

Information

Der Zusatz-Akku kann von der Ladestation nur bei Umgebungstemperaturen < 40 °C aufgeladen werden.

Um den Zusatz-Akku zu laden, gehen Sie wie folgt vor:

1) Den Zusatz-Akku mit der Magnethalterung an der Ladestation befestigen.

KEBA © KEBA 2021

2) Das Ladekabel an die Buchse für 24 V Stromversorgung des Zusatz-Akkus anschließen.
3) Das andere Ende des Ladekabels an die Buchse für 24 V Stromversorgung an der Ladestation anschließen.

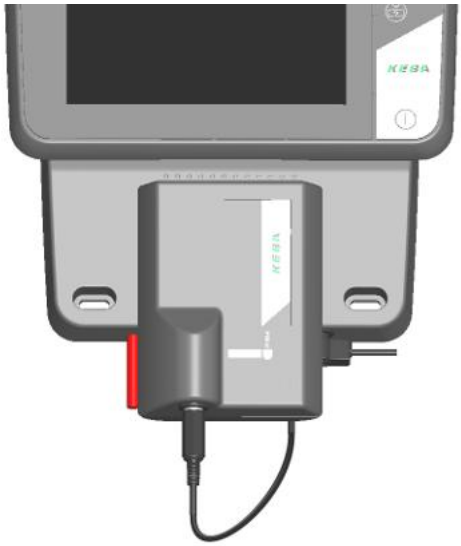


Abb. 17-111: Zusatz-Akku wird an der Ladestation aufgeladen

Der Zusatz-Akku wird geladen.

Folgendes ist unbedingt zu beachten:

- Wenn das Handbediengerät in der Ladestation steckt, den Zusatz-Akku immer vom Handbediengerät trennen.
- Wenn das Handbediengerät in der Ladestation steckt und der Zusatz-Akku am Handbediengerät angeschlossen bleibt/wird, wird der Zusatz-Akku **nicht** geladen.
- Die Ladestation ist nicht gegen einen Rückstrom vom Zusatz-Akku abgesichert. Wenn die externe Versorgung der Ladestation abgeschaltet wird, muss der Zusatz-Akku von der Ladestation getrennt werden, sonst entlädt sich dieser ungewollt.

17.6.3 Technische Daten

Umgebungsbedingungen

Betriebstemperatur:	0 °C bis 40 °C
Lagertemperatur:	
• < 1 Jahr	-20 °C bis +20 °C
• < 3 Monate	-20 °C bis +45 °C
• < 1 Monat	-20 °C bis +50 °C
Ladetemperatur:	0 °C bis 40 °C
Relative Luftfeuchtigkeit (nicht kondensierend):	5 % bis 95 % (nicht kondensierend)

© KEBA 2021

Betriebsbereich:	Innen
Einsatzhöhe:	Max. 2.000 m Seehöhe
Schutzart:	IP54
Verschmutzungsgrad:	2

Spannungen

Ladespannung:	24 V DC (Nennspannungstoleranzbereich 19,2 V DC bis 30 V DC SELV / PELV nach EN 61131-2)
Überspannungskategorie beim Laden:	II
Ausgangsspannung:	14,4 V DC

Betriebs- und Ladezeiten

Typische Betriebszeit:	ca. 3,5 h
Typische Ladezeit für 80 % der Kapazität:	ca. 2 h

Mechanische Eigenschaften

Konstruktion:	Gehäuse aus PPE/PS
Flammwidrigkeit:	UL94-V0
Falltauglichkeit (2 Fälle nach EN 61131-2):	1 m (auf Industrieboden, danach noch mind. Schutzart IP54)

Maße und Gewicht

Höhe:	115 mm
Breite:	93 mm
Tiefe:	115 mm
Gewicht:	382 g

Akku Spezifikationen

Modellbezeichnung:	RRC2054
Batteriekategorie:	Gerätebatterie
Chemische Zusammensetzung:	Lithium-Ionen (Li-Ion)
Konfiguration:	4s1p
Kapazität:	ca. 3,4–3,5 Ah
Wiederaufladbar:	Ja
Austauschbar:	Ja

Verwendete Zelltypen

Zelltyp:	NCR18650GA	INR18650-35E
Zellhersteller:	Panasonic	Samsung SDI
Kapazität:	3,45 Ah	3,40 Ah
Energie:	49,68 Wh	48,96 Wh

KEBA © KEBA 2021

17.7 Rückwand für rückseitige Kabelmontage (nur für CB41x)

Dieses Zubehör für CB41x kann statt der Standard-Rückwand verwendet werden und ermöglicht durch eine Ausnehmung eine rückseitige Verkabelung bei geschlossener Basisstation.

Bestellnummer	Bezeichnung
106482	CB310 UT Set f. Schaltschr.montage

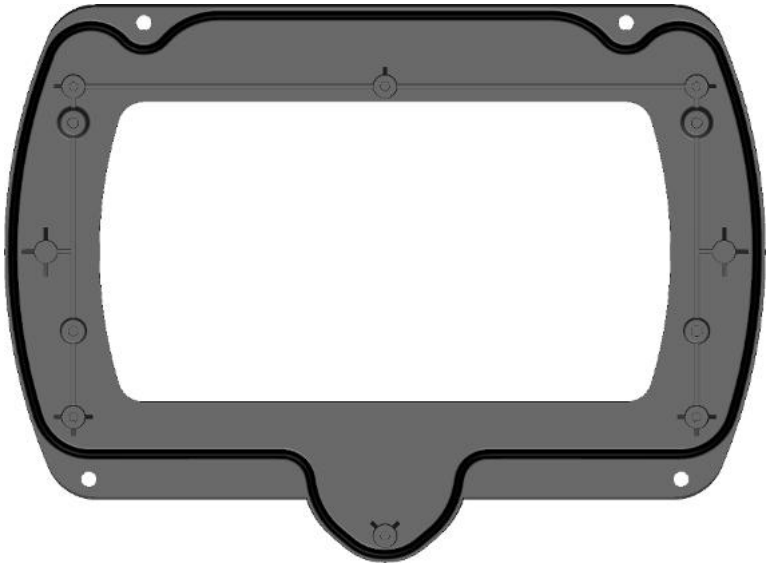


Abb. 17-112: Rückwand für rückseitige Verkabelung

Die Montage dieser Rückwand ist ident mit jener der Standard-Rückwand.

Achtung

Die Montagefläche der Rückwand für rückseitige Verkabelung ist mit einer Dichtung versehen. Um die Dichtheit zu gewährleisten, muss diese auf einer ebenen Fläche montiert werden und der Kabeldurchbruch in der Wand muss kleiner als die Ausnehmung dieser Rückwand sein.

Achtung

Bei der Verkabelung der Basisstation mit dieser Rückwand, muss schaltschrankseitig eine Zugentlastung der Kabel sichergestellt werden.

17.8 Displayschutzglas

Für das Handbediengerät ist folgendes optionales Zubehör zum Schutz des Displays vor Kratzern und Beschädigungen erhältlich:

© KEBA 2021

Bestellnummer	Bezeichnung
140761	Premium Displayschutzglas KeTop T15x

KEBA © KEBA 2021

18 Richtlinien, Normen und Verordnungen

18.1 EU-Richtlinien / Verordnungen

2014/53/EU	RED-Richtlinie
2022/30/EU	Delegierte Verordung
2011/65/EU	RoHS-Richtlinie
2006/42/EG	Maschinenrichtlinie

18.2 Normen zur Überprüfung der Konformität

Zur Überprüfung der Konformität mit den Richtlinien wurden die folgenden rechtlich unverbindlichen europäischen Normen angewendet.

Überprüfung der Konformität mit der RED-Richtlinie

EN 300 328	Breitband-Übertragungssysteme - Datenübertragungsgeräte zum Betrieb im 2,4-GHz-Band - Harmonisierte Norm zur Nutzung von Funkfrequenzen
EN 300 330	Funkanlagen mit geringer Reichweite (SRD) - Funkgeräte im Frequenzbereich 9 kHz bis 25 MHz und induktive Schleifensysteme im Frequenzbereich 9 kHz bis 30 MHz - Harmonisierte EN, die die wesentlichen Anforderungen nach Artikel 3.2 der EU-Richtlinie 2014/53/EU enthält
EN 301 893	5-GHz-RLAN - Harmonisierte EN, die die wesentlichen Anforderungen nach Artikel 3.2 der EU-Richtlinie 2014/53/EU enthält

Überprüfung der Konformität mit der Niederspannungsrichtlinie (laut RED Artikel 3 Absatz 1a)

EN 50364	Produktnorm für die Exposition von Personen gegenüber elektromagnetischen Feldern von Geräten, die im Frequenzbereich von 0 Hz bis 300 GHz betrieben und in der elektronischen Artikelüberwachung (EAS), Hochfrequenz-Identifizierung (RFID) und ähnlichen Anwendungen verwendet werden
EN 62479	Beurteilung der Übereinstimmung von elektronischen und elektrischen Geräten kleiner Leistung mit den Basisgrenzwerten für die Sicherheit von Personen in elektromagnetischen Feldern (10 MHz bis 300 GHz)
EN 62311	Bewertung von elektrischen und elektronischen Einrichtungen in Bezug auf Begrenzungen der Exposition von Personen in elektromagnetischen Feldern (0 Hz - 300 GHz)

© KEBA 2021

Überprüfung der Konformität mit der EMV-Richtlinie (laut RED Artikel 3 Absatz 1b)

EN 61131-2	Speicherprogrammierbare Steuerungen - Teil 2: Betriebsmittelanforderungen und Prüfungen
EN 61000-6-2	Elektromagnetische Verträglichkeit (EMV) - Teil 6-2: Fachgrundnormen - Störfestigkeit für Industriebereiche
EN 61000-6-4	Elektromagnetische Verträglichkeit (EMV) - Teil 6-4: Fachgrundnormen - Störaussendung für Industriebereiche
EN 301 489-1	Elektromagnetische Verträglichkeit (EMV) - Standard für Funkeinrichtungen und -dienste - Teil 1: Gemeinsame technische Anforderungen

Überprüfung der Konformität mit der delegierten Verordnung 2022/30/EU (laut RED Artikel 3 Absatz 3d)

EN 18031-1	Gemeinsame Sicherheitsanforderungen für Funkanlagen (Teil1: Funkanlagen mit Internetanschluss)

Überprüfung der Konformität mit der RoHS-Richtlinie

EN IEC 63000:2018	Technische Dokumentation zur Beurteilung von Elektro- und Elektronikgeräten hinsichtlich der Beschränkung gefährlicher Stoffe

Überprüfung der Konformität mit der Maschinenrichtlinie

EN ISO 13850:2015	Sicherheit von Maschinen - Not-Halt - Gestaltungsleitsätze
EN ISO 13849-1:2015	Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze
EN 60204-1:2018	Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen - Teil 1: Allgemeine Anforderungen
EN ISO 10218-1:2011	Industrieroboter - Sicherheitsanforderungen - Teil 1: Roboter
EN 62061:2021	Sicherheit von Maschinen - Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme

18.3 Sonstige Normen

Folgende rechtlich unverbindliche europäische Normen wurden bei der Produktgestaltung in Teilaspekten mitberücksichtigt.

KEBA © KEBA 2021

Allgemeine Vorgehensweisen und Sicherheitsprinzipien

EN ISO 12100:2010	Sicherheit von Maschinen - Allgemeine Gestaltungsleitsätze - Risikobewertung und Risikominderung

Ausführung des Stopp- bzw. Not-Halt-Schalters

EN ISO 13850:2015	Sicherheit von Maschinen - Not-Halt - Gestaltungsleitsätze
EN 60204-1:2018	Sicherheit von Maschinen - Elektrische Ausrüstung von Maschinen - Teil 1: Allgemeine Anforderungen

Ausführung des Zustimmtasters

EN 60204-1:2018	Sicherheit von Maschinen - Elektrische Ausrüstung von Maschinen - Teil 1: Allgemeine Anforderungen
EN ISO 10218-1:2011	Industrieroboter - Sicherheitsanforderungen - Teil 1: Roboter
EN 60947-1:2007	Niederspannungsschaltgeräte - Teil 1: Allgemeine Festlegungen
EN 60947-5-1:2017	Niederspannungsschaltgeräte - Teil 5-1: Steuergeräte und Schaltelemente - Elektromechanische Steuergeräte
EN 60947-5-8:2021	Niederspannungsschaltgeräte - Teil 5-8: Steuergeräte und Schaltelemente - Drei-Stellungs-Zustimmschalter

Ergonomie

EN 614-1:2006	Sicherheit von Maschinen - Ergonomische Gestaltungsgrundsätze - Teil 1: Begriffe und allgemeine Leitsätze
EN 614-2:2000	Sicherheit von Maschinen - Ergonomische Gestaltungsgrundsätze - Teil 2: Wechselwirkungen zwischen der Gestaltung von Maschinen und den Arbeitsaufgaben

Festigkeit und Dichtheit des Gehäuses

EN 60529:1991	Schutzarten durch Gehäuse
EN 61131-2:2007	Speicherprogrammierbare Steuerungen - Teil 2: Betriebsmittelanforderungen und Prüfungen

© KEBA 2021

Funktional relevante Elektromagnetische Verträglichkeit

EN 61000-6-7	Elektromagnetische Verträglichkeit (EMV) - Teil 6-7: Fachgrundnormen - Störfestigkeitsanforderungen an Geräte und Einrichtungen, die zur Durchführung von Funktionen in sicherheitsbezogenen Systemen (funktionale Sicherheit) an industriellen Standorten vorgesehen sind
EN 61326-3-1	Elektrische Mess-, Steuer-, Regel- und Laborgeräte - EMV-Anforderungen - Teil 3-1: Störfestigkeitsanforderungen für sicherheitsbezogene Systeme und für Geräte, die für sicherheitsbezogene Funktionen vorgesehen sind (Funktionale Sicherheit) - Allgemeine industrielle Anwendungen
EN 61131-6	Speicherprogrammierbare Steuerungen - Teil 6: Funktionale Sicherheit
IEC 61131-2	Industrial-process measurement and control - Programmable controllers - Part 2: Equipment requirements and tests
EN 12895	Flurförderzeuge - Elektromagnetische Verträglichkeit

Weitere relevante Normen und Prinzipien

EN 61131-2:2007	Speicherprogrammierbare Steuerungen - Teil 2: Betriebsmittelanforderungen und Prüfungen
EN 61010-1:2010	Sicherheitsbestimmungen für elektrische Mess-, Steuer-, Regel- und Laborgeräte - Teil 1: Allgemeine Anforderungen
EN IEC 61010-2-201:2018	Sicherheitsbestimmungen für elektrische Mess-, Steuer-, Regel- und Laborgeräte - Teil 2-201: Besondere Anforderungen für Steuer- und Regelgeräte (ohne funktionale Sicherheit)
GS-ET-07	Kabellose Steuereinrichtungen für Sicherheitsanforderungen an Maschinen
GS-ET-22	Elektromechanische Zustimmungsschalter und Zustimmungseinrichtungen mit und ohne Anlaufsteuerung
EN 62745:2017	Sicherheit von Maschinen - Anforderungen für kabellose Steuerungen an Maschinen
EN 61508-1:2010	Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 1: Allgemeine Anforderungen
EN 61508-2:2010	Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme

KEBA © KEBA 2021

EN 61508-3:2010	Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 3: Anforderungen an Software
EN ISO 3691-4:2020	Flurförderzeuge - Sicherheitstechnische Anforderungen und Verifizierung – Teil 4: Fahrerlose Flurförderzeuge und ihre Systeme
EN 61784-3-3:2017	Industrielle Kommunikationsnetzwerke - Profile - Teil 3-3: Funktional sichere Übertragung bei Feldbussen - Zusätzliche Festlegungen für die Kommunikationsprofilfamilie 3

18.4 Verordnungen

Verordnung (EG) Nr. 1907/2006	REACH EU-Chemikalienverordnung

Information

Informationspflicht aus der REACH Verordnung

Um der Informationspflicht nach Artikel 33 der REACH Verordnung nachzukommen, werden detaillierte Informationen zu den Inhaltsstoffen / SVHC auf unserer Internetseite bereitgestellt. Das Dokument kann auf https://support.keba.com unter "Verordnungen" heruntergeladen werden.

18.5 Normen für den amerikanischen Markt

Für den amerikanischen Markt wurden die folgenden Normen berücksichtigt.

UL Prüfung für Industrielle Steuerungseinrichtungen

UL/IEC 61010-2-201	Requirements for Control Equipment, including Programmable Logic Controllers (PLC's) and applicable requirements from UL/IEC61010-1
UL 3100	Automated Guided Vehicles (AGVs)

Code of Federal Regulations, Titel 47, Teil 15

CFR 47, Part 15	Radio Frequency Devices

Folgende Funkmodule sind im Produkt verbaut:

Bezeichnung	FCC-ID	T15xWL	CB 4xx
RFID Uni Module	U870008	x	
Sparklan WPEQ	RYK-261ACNBT	x	
Ublox NINA B112	XPYNINAB1	x	x
Lantronix Xpico	R68XPICO200		x

© KEBA 2021

Bezeichnung	FCC-ID	T15xWL	CB 4xx
WAL R1	U870009	x	x

Folgender Hinweis gilt für den amerikanischen Markt:

The device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1) this device may not cause harmful interference, and
2) this device must accept any interference received, including interference that may cause undesired operation.

This device is labelled with an FCC ID number. If this label is not visible when installed in an end device, the outside of the device MUST also display a label referring to the enclosed module.

e.g.

“Contains FCC ID: U870xxx” (KEBA Product xxx)

Information

- Changes or modifications not expressly approved by the manufacturer could void the user’s authority to operate the equipment.

18.6 Normen für den kanadischen Markt

Für den kanadischen Markt wurden die folgenden Normen berücksichtigt.

Radio Standards Specification RSS-210, Issue 8

RSS-210 Issue 8	Licence-exempt Radio Apparatus

Folgende Funkmodule sind im Produkt verbaut:

Bezeichnung	IC-ID	T15xWL	CB 4xx
RFID Uni Module	20800-RFIDUNI	x	
Sparklan WPEQ	6158A-261ACNBT	x	
Ublox NINA B112	8595A-NINAB1	x	x
Lantronix Xpico	3867-XPICO200		x
WAL R1	20800-WALR1MOD	x	x

EN: This device complies with Industry Canada's licence-exempt RSSs. Operation is subject to the following two conditions:

1) This device may not cause interference, and
2) this device must accept any interference, including interference that may cause undesired operation of the device.

KEBA © KEBA 2021

FR: Le présent appareil est conforme aux CNR d'Industire Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

1) L'appareil ne doit pas produire de brouillage;
2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage es susceptible d'en compromettre le fonctionnement.

18.7 Normen für den japanischen Markt

Folgende Funkmodule sind im Produkt verbaut:

Bezeichnung	MIC-ID	T15xWL	CB 4xx
RFID Uni Module	AC-21044	x	
Sparklan WPEQ	020-170122	x	
Ublox NINA B112	204-610006	x	x
Lantronix Xpico	020-170133		x
WAL R1	203-JN1257	x	x

Sehen Sie dazu auch

Certificate_Japan u-blox NINA-B111 NINA-B112 [} 258]

© KEBA 2021

RCB Japan
Königswinkel 10
D-32825 Blomberg, Germany
Phone: +49 (0) 5235 9500-75
Fax: +49 (0) 5235 9500-28
www.phoenix-testlab.de

Type Certification

No: 17-112434

for
Specified Radio Equipment in Japan

PHOENIX TESTLAB GmbH, operating as a Registered Certification Body (RCB ID: 204) with respect to Japan, declares that the listed product complies with the Technical Regulations Conformity Certification of Specified Radio Equipment (ordinance of MPT N°. 37, 1981), Article 2, Paragraph 1, Item 19.

Product description:	**Bluetooth Low-energy Module with Passive NFC-tag Functionality**
Trademark:	**ublox**
Family name:	**NINA-B1**
Model name:	**NINA-B111 ; NINA-B112**
Serial No:	--
Software Release No:	--
Type of emissions:	F1D
Frequency and power:	BT (LE): 2402~2480 MHz; 40 ch; 2.80 mW (1 Mbit/s) BT (LE): 2402~2480 MHz; 40 ch; 1.70 mW (2 Mbit/s)

Manufacturer:	Flextronics International GmbH
Address:	Friesacher Str. 3
City:	9330 Althofen
Country:	Austria

This certificate is granted to:

Certificate holder:	u-blox AG
Address:	Zürcherstrasse 68
City:	8800 Thalwil
Country:	Switzerland

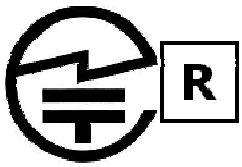
This certificate has 2 annexes.

PHOENIX TESTLAB GmbH
Königswinkel 10
32825 Blomberg
Tel. 0 52 35 / 95 00-0
Fax 0 52 35 / 95 00-10

Blomberg, Jun. 18, 2018
Place, Date

Detlef Lachmund

- The validity of this certificate is limited to products, which are equal to the one examined in the type-examination.
- When the holder of this certificate is placing the product on the Japanese market, the product must be affixed with the following Specified Radio Equipment marking:



204-610006

Remarks and observations:

The following conditions are applicable:

Antenna name	Manufacturer	Comment	Gain [dBi]
u-blox NINA Antenna	ProAnt	SMD PIFA antenna on NINA-B112	3 dBi @ 2.4 GHz
FlatWhip-2400	ProAnt	Monopole, SMA/RSMA	3 dBi @ 2.4 GHz
InSide-2400	ProAnt	Patch, 10cm cable/U.FL	3 dBi @ 2.4 GHz
Ex-IT 2400 -SMA 28-001 -RP-SMA 28-001 -MHF 28-001	ProAnt	Monopole, SMA RSMA 10 cm cable/U.FL	3 dBi @ 2.4 GHz
Ex-IT 2400 -SMA 70-002 -RP-SMA 70-002	ProAnt	Monopole, SMA RSMA	3 dBi @ 2.4 GHz
GW26.0111.HT	Taoglas	Single-band monopole antenna	3 dBi @ 2.4 GHz

Documentation lodged for the type examination:

Testreports:

- PHOENIX Testlab GmbH: F161370E1, Aug. 15, 2016
- PHOENIX Testlab GmbH: F172433E1, Jun. 14, 2018

Product documentation:

- Block Diagram
- Bill of Materials
- Photos
- User Manual
- Circuit Diagram
- Placement Drawings
- Antenna Specifications

Technical standards and specifications

The product complies with:

Ordinance Regulating Radio Equipment
- Chapter I, General Provisions
- Chapter II, Transmitting Equipment
- Chapter III, Receiving Equipment
- Chapter IV, Article 49.20

Technical features and characteristics:

The product includes the following features and characteristics:

- Modulation method(s):
  Bluetooth LE: GFSK for 1 Mbit/s
  Bluetooth LE: GFSK for 2 Mbit/s

Please note the following points:

1. A person (including a legal person) who was granted the Type Certification (hereafter referred to as "certification dealer" is obliged to prepare and maintain the examination records by Radio Law, Article 38-25, Paragraph 2 and Certification Regulations.
2. Please report to us without delay if any item in the application for this Type Certification is to be changed. The Type Certification will become invalid if there is any discrepancy between the contents of the application documents and the fact.
3. Please keep all records of complaints against this certified equipment (all those reported to suppliers), and provide them to us for our reference upon request.
4. Please take necessary measures against any complaints concerning insuffiency of the equipment or service that influences conformity with technical regulations. Please keep all records of measures you have taken and provide them to us for our reference.
5. Market research can be conducted concerning this Type Certification. In such a case, the necessary testing tools should be submitted upon request.

♦ **Radio Law, Article 38-25**

1. A person who was granted the Type Certification (hereafter referred to as "certification dealer") by a registered certification agency shall, when dealing a specified radio equipment based on the construction type pertaining to said Type Certification (hereafter referred to as "certified construction type"), ensure that said radio equipment confirms to said certified construction type).
2. A certification dealer shall conduct an examination on the specified radio equipment stated in the preceding paragraph, and prepare and maintain the examination records in accordance with the applicable ministerial ordinance of the Ministry of Internal Affairs and Communications.

♦ **Certification Regulations, Article 19**

1. The items of examination record specified under Article 38-25, Paragraph 2 of Radio Law shall include followings:
    1) Type Certification number pertaining to the examination
    2) Date and location that the examination took place
    3) Name of the person who conducted and is in charge of the examination
    4) Name of the specified Radio Equipment which was examined
    5) Method of Examination
    6) Result of Examination
2. The examination record in the preceding paragraph must be stored for 10 years.
3. The examination record in the preceding paragraph can be stored by using the recording media of electromagnetic record. In this case, the stored electromagnetic record must be able to be displayed at once with computer or other devices when necessary.

19 EU-Konformitätserklärung

KEBA
Automation by innovation.

EG-/EU-Konformitätserklärung
EC/EU Declaration of Conformity

CE

KEBA Industrial Automation GmbH
Reindlstraße 51
A- 4040 Linz
AUSTRIA

Wir bestätigen, dass das (die) nachfolgend bezeichnete(n) Produkt(e)
We declare that the following product(s)

Type: **KeTop T15xWL / C15xWL**
KeTop CB4xx

Beschreibung: Kabelloses Handterminal System mit 3-stufigen Zustimmtaster und Not-Halt
Description: Wireless Teach Pendant System with 3-position Enabling Device and E-Stop

Variante(n): **Mat.Nr. KeTop T15xWL / C15xWL:**
Variant(s):

124390	124391	124392
124393	124394	124395
124396	124397	124398
124504	126183	126252
126253	126256	126503
126510	126688	126808
128756	128757	128758
129264	129278	130076
130611	130612	131051
131494	131496	131801
131894	131963	132204
132998	133115	133197
133303	133399	133474
133726	135368	135797
136682	136848	138166

Mat.Nr. KeTop CB4xx:

124399	124400	124401
124295	124296	126054
126055	126257	130077
130619	130620	131054
131895	132999	133199
133296	133317	133472
133473	133760	135392
136684	138180	

IA_KeTop_T15x-CB410-WL_dt-en15.docx

© KEBA 2021

KEBA
Automation by innovation.

den Schutzbestimmungen folgender europäischer Richtlinie(en) und delegierter Verordnung(en) entspricht/entsprechen:

is (are) in conformity with the following relevant Union harmonization legislation(s) and delegated regulation(s):

- **2006/42/EC**
- **2014/53/EU + (EU) 2022/30**
- **2011/65/EU**

Folgende einschlägige harmonisierte Norm(en) wurde(n) der Konformitätsvermutung zur Richtlinie 2006/42/EG für die Sicherheitsfunktionen zugrunde gelegt:

Following relevant harmonized standard(s) has/have been used to give presumption of conformity to the directive 2006/42/EC for the safety functions:

- **EN ISO 13849-1:2023**
- **EN IEC 62061:2021 + A1:2024**
- **EN ISO 13850:2015**
- **EN ISO 10218-1:2011**
- **EN 60204-1:2018**
- **EN 62745:2017 + A11:2020**

Folgende benannte Stelle hat das Baumusterprüfverfahren nach Anhang IX der Maschinenrichtlinie 2006/42/EG durchgeführt:

A type examination according Machinery Directive 2006/42/EC annex IX was performed by the certification body:

TÜV Rheinland Industrie Service GmbH
Am Grauen Stein
51105 Köln / Germany
Notified Body for Machinery, NB 0035
Type examination: 01/205/5833.03/25

Folgende einschlägige harmonisierte Norm(en) wurde(n) der Konformitätsvermutung zur Richtlinie 2014/53/EU und ergänzender delegierter Verordnung (EU) 2022/30 zugrunde gelegt:
Following relevant harmonised standard(s) has (have) been used to give presumption of conformity to the Directive 2014/53/EU and supplementary delegated regulation (EU) 2022/30:

- **EN 300 328 V2.2.2**
- **EN 300 330 V2.1.1**
- **EN 301 893 V2.1.1**
- **hEN 18031-1:2025**

Der Schutz der Gesundheit und Sicherheit gemäß Art. 3 (1) a, 2014/53/EU werden durch die Einhaltung der zur Richtlinie 2014/35/EU harmonisierte(n) Norm(en) nachgewiesen:

The protection of health and safety referred to Art. 3 (1) a, 2014/53/EU is assured by the compliance with the applicable parts of the following harmonized european standards according to 2014/35/EU.

- **EN 50364:2010**
- **EN 62479:2010**

IA_KeTop_T15x-CB410-WL_dt-en15.docx

KEBA © KEBA 2021

KEBA
Automation by innovation.

- **EN 62311:2008**

Ein angemessenes Niveau an elektromagnetischer Verträglichkeit gemäß Art. 3 (1) b, 2014/53/EU wird durch Anwendung der zur Richtlinie 2014/30/EU harmonisierte(n) Norm(en) nachgewiesen:

An adequate level of electromagnetic compatibility referred to Art. 3 (1) b, 2014/53/EU is assured by the compliance with the applicable parts of the following harmonized european standards according to 2014/30/EU.

- **EN 61131-2:2007**
- **EN 61000-6-2:2005 + AC:2005**
- **EN 61000-6-4:2007 + A1:2011**
- **EN 301 489-1 V1.9.2**

Folgende einschlägige harmonisierte Norm/en wurde/n für die Konformiätsvermutung mit der Richtlinie 2011/65/EU zugrunde gelegt:

Following relevant harmonized standard/s was/were used as the basis for the presumption of conformity with the directive 2011/65/EU:

- **EN IEC 63000:2018**

Wichtige Hinweise:

Die alleinige Verantwortung für die Ausstellung dieser Konformitätserklärung trägt KEBA.

Bei einer nicht mit KEBA abgestimmten Änderung des Produkts verliert das Produkt die Konformitätsvermutung.

Die deutschsprachige Teil dieses Dokumentes ist die Originalversion, alle anderssprachigen Teile wurden aus dem Original-Text übersetzt.

Bevollmächtigter für die Zusammenstellung der technischen Unterlagen ist KEBA Industrial Automation GmbH, Reindlstraße 51, A-4040 Linz.

Important notes:

This declaration of conformity is issued under the sole responsibility of KEBA.

The product loses the presumption of conformity in case of any modification on the product without KEBA's consent.

The German-language part of this document is the original version, all other language parts have been translated from the original text.

Authorised to compile the technical file is KEBA Industrial Automation GmbH, Reindlstraße 51, A-4040 Linz.

Linz, 2025-07-17
Ort, Datum
Place, Date

Bernhard Lehner
Head of Product Compliance

IA_KeTop_T15x-CB410-WL_dt-en15.docx

© KEBA 2021

20 Anhang: Inbetriebnahme

In diesem Kapitel werden die Inbetriebnahmeschritte, wie teilweise in den gleichnamigen Kapiteln beschrieben, aufgelistet.

1) Montieren der Basisstation.
2) Verkabeln der Basisstation.
3) Konfiguration der Basisstation: Einstellen der Box-ID und bei Verwendung eines Bedienbereichs diesen über die DIP-Switches einstellen.
4) Schließen und Verschrauben der Basisstation.
5) Validieren der Basisstation.
6) Optional: Montieren und Verkabeln der Ladestation.
7) Anschließen des Akkus (im Auslieferzustand ist der Anschlussschacht geöffnet).
8) Schließen und Verschrauben des Anschlussschachts.
9) Vollständiges Aufladen des Handbediengeräts an einem Ladegerät oder der Ladestation (min. 2 h).
10) Handbediengerät mit der Basisstation verbinden ("Pairing").
11) Gerätekonfiguration ("DeviceConfig") starten.
12) Mittels "Basestation" Konfigurieren der Basisstation.
13) Mittels "Network" Einstellen des gewünschten Verhaltens ("Modus") und Konfigurieren der Netzwerkeinstellungen der Geräte.
14) Konfigurieren des Handbediengeräts (z.B. Fernzugriff, IT-Sicherheitseinstellungen).
15) Installieren und Konfigurieren der gewünschten Verbindungsprotokolle am Handbediengerät.
16) Projektieren der Visualisierung.
17) Visualisierungsapplikation auf das Handbediengerät laden und starten.

KEBA © KEBA 2021

21 Anhang: Sicherheit von Maschinen

Richtlinien der Europäischen Union

Ein wesentliches Ziel der Europäischen Union ist die Realisierung eines europäischen Binnenmarktes, und damit verbunden der freie Warenverkehr. Das bedeutet, dass quantitative Einfuhrbeschränkungen von Waren zwischen den Mitgliedstaaten verboten sind.

Ausgenommen davon sind Waren, die die Sicherheit von Personen oder der Umwelt gefährden. Solche Produkte können von Mitgliedsstaaten auf ihrem Hoheitsgebiet unterbunden werden. Um auch für diese Produkte den freien Warenverkehr sicherzustellen werden die nationalen Sicherheitsbestimmungen der Mitgliedsstaaten mittels Richtlinien der Europäischen Union vereinheitlicht.

Diese Richtlinien gibt es für eine Reihe von Produktklassen, wie z.B. Maschinen, Medizinprodukte oder auch Spielwaren. Aber auch für weitere gemeinsame Sicherheitsaspekte von Produkten, wie Schutz vor Elektrizität, Explosionsschutz oder Elektromagnetische Verträglichkeit wurden entsprechende Richtlinien erarbeitet. Die Richtlinien richten sich an die Mitgliedsstaaten, welche diese in den jeweiligen nationalen Gesetzen umsetzen müssen. Die Richtlinien haben daher Gesetzescharakter.

Mit der „CE“-Kennzeichnung bescheinigt der Hersteller alle Verpflichtungen der auf das Produkt zutreffenden EU-Richtlinien erfüllt zu haben. Das CE-Zeichen, welches der Hersteller selbst auf die Produkte aufbringt, ist der „Reisepass“ innerhalb der EU und für die überwachenden Behörden bestimmt.

Ergänzend dazu kann von unabhängigen, akkreditierten Zertifizierungsstellen die Konformität mit den EU-Richtlinien überprüft und dies mit einer EG-Baumusterbescheinigung bestätigt werden.

Für Handbediengeräte ist neben der Maschinenrichtlinie (MRL 2006/42/EG) aufgrund des Einbaus von Funkmodulen auch die Funkanlagen Richtlinie (RED RL 2014/53/EU) anzuwenden.

Sicherheit von Maschinen

Überall, wo an der Maschine auftretende Fehler Personenschaden oder große Materialschaden verursachen können, müssen zusätzliche Maßnahmen getroffen werden, die auch im Fehlerfall einen sicheren Betriebszustand des Gesamtsystems gewährleisten. Als Maschine gilt laut Maschinenrichtlinie (MRL) "eine Gesamtheit von miteinander verbundenen Teilen oder Vorrichtungen, von denen mindestens eines beweglich ist“. Die Richtlinie besagt auch, dass „durch die Bauart der Maschine gewährleistet sein muss, dass Betrieb, Rüsten und Wartung bei bestimmungsgemäßer Verwendung ohne Gefährdung von Personen erfolgen.“

Obwohl das Handbediengerät selbst keine Maschine im engeren Sinn ist, erfüllt es doch wesentliche Aufgaben zur Gewährleistung von Sicherheitsfunktionen einer Maschine oder Anlage, an die es angeschlossen ist.

© KEBA 2021

Das Handbediengerät verfügt z.B. über die Sicherheitsfunktionen „Stoppen im Notfall“ und über einen Zustimmtaster für Bedienung in Sonderbetriebsarten, und ist somit ein „Sicherheitsbauteil“ im Sinne der Maschinenrichtlinie.

Sicherheitsbauteile, also Teile deren Ausfall oder Fehlfunktion die Sicherheit von Personen im Gefahrenbereich der Maschine gefährden, fallen ausdrücklich in den Anwendungsbereich der Maschinenrichtlinie. Wesentliche Anforderungen der Maschinenrichtlinie an den Hersteller einer Maschine oder Anlage sind:

- Durchführung einer Gefahren- und Risikoanalyse
- Befolgung der Grundsätze für die Integration der Sicherheit
- Erstellung und Verwahrung einer Technischen Dokumentation
- Lösungen gemäß dem Stand der Technik
- Konformitätsvermutung mittels harmonisierter Normen
- Aufbringung der CE-Konformitätskennzeichnung

Für Sicherheitsbauteile gelten im Wesentlichen die gleichen Anforderungen. Für Sicherheitsbauteile muss nachgewiesen werden, dass ein Ausfall oder eine Fehlfunktion nicht möglich ist, oder, dass eine Fehlfunktion nicht zu einer gefährlichen Situation führt.

21.1 Risikobeurteilung

Der Hersteller einer Maschine ist verpflichtet, eine Risikobeurteilung seiner Maschine durchzuführen. Die Risikobeurteilung besteht aus einer Gefährdungsanalyse und einer Risikobewertung. Es ist die Maschine in allen Lebensphasen und Betriebsarten zu analysieren, und alle möglichen auftretenden Gefahren sind zu dokumentieren. Dies geschieht ohne Berücksichtigung von eventuellen Schutzeinrichtungen.

Als nächster Schritt wird für jede erkannte Gefahr ein Schutzziel formuliert, und anschließend eine oder mehrere Schutzmaßnahme(n) zu Erreichung des Schutzzieles definiert.

Weitere Details zur Vorgangsweise bei der Durchführung der Gefahren- und Risikoanalyse sowie Listen von häufig anzutreffenden Gefährdungen finden sich in folgenden Normen:

- EN ISO 12100:2010 „Sicherheit von Maschinen-Grundbegriffe - Allgemeine Gestaltungsleitsätze, Risikobeurteilung und Risikominderung“

21.2 Grundsätze für die Integration des KeTops

Im Anhang I, Kap. 1.1.2 der MRL 2006/42/EG schreibt die MRL eine klare Vorgangsweise und Reihenfolge für die Auswahl der Schutzmaßnahmen vor:

KEBA © KEBA 2021

Beseitigen oder Minimieren der Gefahren

Dies geschieht bereits durch die Konstruktion der Maschine. Unter diese Maßnahmen fallen z.B.:

- Reduktion von auftretenden Energien (Kräfte, Drehzahlen, Spannungen…), soweit dies möglich ist
- Vermeidung unnötiger Scherstellen oder scharfen Kanten
- Vermeidung von Fehlbedienungen durch ergonomische und logische Gestaltung von Bedienvorrichtungen
- Vermeidung gefährlicher Materialien und Verbrauchsstoffe

Treffen von Schutzmaßnahmen gegen Gefahren, die sich nicht beseitigen lassen

Unter diese Maßnahmen fallen z.B.:

- Trennende Schutzeinrichtungen (Umwehrungen, Gehäuse, Schutzgitter)
- Nicht trennende Schutzeinrichtungen (Lichtschranken zur Abschaltung der Gefahren)
- Steuerungstechnische Schutzeinrichtungen (Zustimmtaster, Zweihandschaltungen, Drehzahlüberwachungen…)

Unterrichtung des Benutzers über Restgefahren

Diese letzte der drei Möglichkeiten wird angewendet, wenn trotz der ersten beiden Punkte Restgefahren bestehen bleiben. Unter diese Maßnahmen fallen z.B.:

- Warnhinweise
- Schulungen und organisatorische Maßnahmen
- Verwendung persönlicher Schutzausrüstung

21.3 Technische Unterlagen

Die technischen Unterlagen beinhalten alle Dokumente, welche zum Nachweis der Sicherheit der Maschine / des Sicherheitsbauteils erforderlich sind. Das sind z.B.:

- Gesamtplan der Maschine oder des Sicherheitsbauteils inklusive Steuerkreispläne
- Gefahren- und Risikoanalyse
- Berechnungen
- Versuchs- und Testergebnisse
- Liste der grundlegenden für die Maschine anzuwendenden Sicherheitsanforderungen der MRL und Beschreibung der Lösungen
- Angewandte Normen

© KEBA 2021

- Bedienungs- und Betriebsanleitungen

Die Technische Dokumentation muss noch bis mindestens 10 Jahre nach Auslieferung des letzten Produktes aufbewahrt werden, und in einem Schadensfall innerhalb einer Frist von wenigen Tagen vorgelegt werden.

21.4 Stand der Technik

Darunter werden technische Möglichkeiten zu einem bestimmten Zeitpunkt verstanden, welche auf gesicherten Erkenntnissen von Wissenschaft und Technik basieren. Der Stand der Technik beinhaltet auch, dass er wirtschaftlich durchführbar ist, d.h., von der Mehrheit in dem betreffenden industriellen Sektor geleistet werden kann.

Stand der Technik ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung der Maßnahme im Hinblick auf die angestrebten Ziele (z.B. der Ziele des Arbeitsschutzes, des Umweltschutzes, der Sicherheit für Dritte, der Wirtschaftlichkeit: Also allgemein zur Erreichung eines allgemein hohen Niveaus bezogen auf die zu beachtenden Aspekte) insgesamt gesichert erscheinen lässt.

Der Stand der Technik kann sich unabhängig von den Normen weiterentwickeln.

21.5 Konformitätsvermutung mit harmonisierten Normen

Die Europäischen Richtlinien beinhalten hauptsächlich allgemeine Anforderungen an die Sicherheit von Produkten, jedoch keine Realisierungsdetails. Hierfür sind die europäischen Normungsinstitute zuständig, welche für konkrete sicherheitstechnische Problemstellungen oder bestimmte Produktklassen Vorschläge für die Umsetzung liefern. Normen, bei denen davon ausgegangen wird, dass sie die Anforderungen der Richtlinien treffen und sinngemäß richtig umsetzen, werden als „harmonisierte Normen“ aufgelistet. Bei weitem nicht alle erhältlichen Normen sind jedoch harmonisiert.

Ein Hersteller kann durch Anwendung und Umsetzung von harmonisierten Normen die Konformitätsvermutung des jeweiligen Produktes aussprechen. Trotzdem sind die Normen, im Gegensatz zu den Richtlinien, nicht rechtlich verpflichtend. Das bedeutet, dass der Hersteller auch andere Lösungen, als die in den Normen beschriebenen, in Betracht ziehen darf. Allerdings müssen diese Lösungen mindestens das gleiche Sicherheitsniveau wie die relevanten Normen erreichen und den Anforderungen der zutreffenden Richtlinien genügen.

21.6 Auswahl von Performance Level und Kategorie nach EN ISO 13849-1

Die Maschinenrichtlinie fordert, dass ein Defekt in der Logik des Steuerkreises, oder aber auch eine Störung oder Beschädigung desselben, nicht zu einer gefährlichen Situation führen darf. Dieser allgemeine Ansatz wird in der EN ISO 13849-1 „Sicherheitsbezogene Teile von Maschinensteuerungen“

KEBA © KEBA 2021

konkretisiert, welche für sicherheitsrelevante Steuerungsteile Performance Levels (PL a bis e) definiert. Der PL ist abhängig von der Kategorie, dem $MTTF_D$-Wert sowie vom Diagnoseabdeckungsgrad (DC_{avg}) der jeweiligen Sicherheitsschaltung.

Gleich wie in der Vorgängernorm EN 954-1 beschreibt die Kategorie die Struktur der Sicherheitsfunktionen. Neu hinzugekommen ist der Performance Level (PL) welcher die Ausfallswahrscheinlichkeit und die Fehlererkennbarkeit der Sicherheitsfunktion beschreibt.

Die Auswahl des PL erfolgt vom Hersteller der Maschine abhängig vom tatsächlichen Gefahrenpotential, welche anhand der Gefahren- und Risikoanalyse ermittelt wird. Bei Gefahren, welche irreversible Verletzungen oder Tod zur Folge haben können, ist üblicherweise mindestens PL d erforderlich.

Die zum PL angegebene Kategorie gibt Auskunft ob

- das System 1-kanalig gestaltet wurde und ein Fehler somit zum Verlust der Sicherheit führt, die Bauteilverfügbarkeit jedoch hoch ist (Kategorie 1)
- das System 1-kanalig gestaltet wurde, und ein Fehler somit zum Verlust der Sicherheit führt, der Fehler jedoch durch das System erkannt und in irgendeiner Form angezeigt wird (Kategorie 2)
- oder das System 2-kanalig gestaltet wurde und ein Fehler nicht zum Verlust der Sicherheit führt (Kategorie 3) oder
- das System 2-kanalig gestaltet wurde und auch eine Anhäufung von mehreren Fehlern nicht zum Verlust der Sicherheit führt (Kategorie 4).

Wichtig ist in diesem Zusammenhang auch, dass ab Kategorie 3 einzelne Fehler rechtzeitig erkannt werden müssen, um eine Fehleranhäufung, welche schließlich zum Sicherheitsverlust führen kann, zu vermeiden

Fehler, welche erkannt werden müssen, sind bei elektrischen und elektronischen Systemen z.B. Querschlüsse zwischen den Kreisen, Unterbrechungen, Kurzschlüsse oder verklebte Kontakte. Häufig werden zur Erkennung von Fehlern in den einzelnen Sicherheits-Kreisen spezielle zertifizierte Sicherheits-Schaltgeräte eingesetzt, welche bereits einen bestimmten PL aufweisen. Der für die Sicherheitsfunktion notwendige Gesamt-PL wird jedoch nur dann erreicht, wenn auch die Beschaltung mit den zugehörigen Kreisen lt. Produktbeschreibung für den jeweiligen PL umgesetzt wurde, und der PL aller zur Sicherheitsfunktion beitragenden Komponenten berücksichtigt wurde.

Der PL muss daher immer für eine gesamte Sicherheitsfunktion aus den einzelnen Komponenten oder Bauteilen berechnet werden.

Eine Anleitung zur vereinfachten Ermittlung des PL für eine Sicherheitsfunktion aus mehreren Komponenten gibt die Norm EN ISO 13849-1 Kapitel 6.3 und die Anhänge H und I.

Zu beachten ist, dass bei einer Serienschaltung von Sicherheits-Komponenten, diejenige mit dem niedrigste PL in der Sicherheitsfunktion den PL der Sicherheitsfunktion bestimmt. So ergibt eine Sicherheitsfunktion, zusammengesetzt aus 3 Komponenten mit Kategorie 4 PL e, Kategorie 3 PL d und der dritten Komponente mit Kategorie 2 PL c einen PL c für die gesamte Si-

© KEBA 2021

cherheitsfunktion. Wichtig dabei ist weiters, dass ein Fehler den Verlust der Sicherheit zur Folge hat, obwohl Kategorie 4 PL e Komponenten in der Sicherheitsfunktion integriert sind, da eine der verwendeten Komponente nur Kategorie 2 aufweist.

Bei Verkettung mehrerer PLs kann sich der Gesamt-PL verringern. Siehe Kapitel 6.3 EN 13849-1.

Der Nachweis, dass ein Fehler nicht zum Verlust der Sicherheit führt, kann mit Hilfe einer FMEA (Failure Mode and Effects Analysis) erfolgen, bei der alle möglichen anzunehmenden Fehler theoretisch oder auch praktisch durchgespielt werden und gezeigt wird, dass den Anforderungen der Kategorie genüge getan ist.

21.7 Anwendung von Handbediengeräten in Sonderbetriebsarten

Bei der manuellen Steuerung von Maschinen in Sonderbetriebsarten, wo die Sicherheit vom rechtzeitigen Reagieren des Bedienpersonals abhängt, ist es unbedingt erforderlich, dass der Bedienbereich vom Bediener eingesehen werden kann. Das Handbediengerät bietet hier den Vorteil, dass damit sehr nahe an den Bedienbereich herangetreten werden kann. Gleichzeitig steigt mit der Mobilität die Missbrauchsgefahr dadurch, dass mit dem Handbediengerät auch an entfernteren Orten, wo der Bedienbereich nicht mehr wahrgenommen werden kann, bewusst oder unbewusst Maschinenbewegungen in Gang gesetzt werden können. Der Betreiber der Maschine hat daher durch Auswahl der entsprechenden Kabellänge des Handbediengeräts für den richtigen Kompromiss aus notwendiger Flexibilität und einer zumutbaren Arbeitsbereichsbeschränkung zu finden. Bei Funk-Handbediengeräten ist eine Arbeitsbereichseinschränkung durch das Kabel nicht möglich, daher sind bei diesen Handbediengeräten zusätzliche technische Lösungen notwendig.

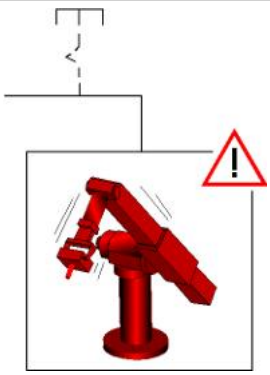
Wird die Maschine oder Anlage mit dem Handbediengerät betrieben, ist darauf zu achten, dass die Bedienung zu diesem Zeitpunkt ausschließlich durch das Handbediengerät und von keinem anderen Punkt der Anlage aus möglich ist. Der Gefahrenbereich darf nur von derjenigen Person betreten werden, welche das Handbediengerät bedient. Sollte es notwendig sein, dass mehr als eine Person gleichzeitig im Gefahrenbereich arbeiten, benötigt jede anwesende Person einen Zustimmtaster, und die Bewegung darf nur freigegeben werden, wenn alle Zustimmtaster betätigt werden.

21.8 Hinweise zum Schalter für das Stillsetzen im Notfall ("Not-Halt")

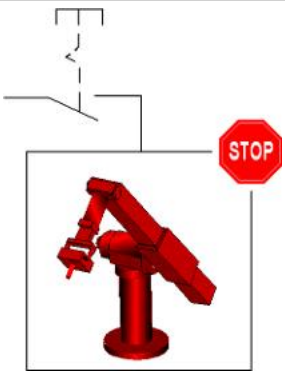
Theoretisch sollte eine perfekt konstruierte Maschine keinen Not-Halt benötigen, da die Maschinenrichtlinie fordert, dass eine Maschine in allen Lebensphasen und Betriebsarten sicher ist. Aus der Praxis weiß man jedoch, dass es trotz aller Vorsichtsmaßnahmen immer wieder zu unvorhersehbaren Situationen kommt. Um in diesen Fällen ein rasches Stillsetzen der Maschine zu ermöglichen, bzw. die Gefahr zu bannen, wird an den meisten Maschinen ein Not-Halt vorgesehen.

KEBA © KEBA 2021

Wie aus der nachfolgenden Abbildung ersichtlich ist, befindet sich eine Maschine aus Sicht des Not-Halts ständig im gefährlichen Zustand, solange dieser nicht betätigt ist.



Not-Halt in Ruhestellung (nicht gedrückt)



Not-Halt gedrückt

Der Not-Halt darf daher nicht als vorwiegende Sicherheits-Einrichtung dienen, sondern ist ausschließlich zur Abdeckung von eventuellen Restrisiken vorgesehen.

Als primäre Sicherheits-Einrichtung sollten stattdessen, abhängig von der Betriebsart, z.B. verriegelnde Schutztüren, Lichtschranken, Zweihandschalter oder Zustimmtaster angewendet werden.

Mit der Betätigung des Not-Halt Schalters muss die gesamte Maschine oder alle zu einer Anlage zusammen geschalteten Maschinen in einen sicheren Zustand übergeführt werden, z.B. durch Abschaltung der Energie der gefährdenden Antriebe (Stopp-Kategorien 0 oder 1 nach EN 60204-1).

Das Entriegeln des Not-Halt Schalters darf keinen unkontrollierten Wiederanlauf der Maschine bewirken.

Unabhängig davon, ob auf einem Handbediengerät ein Not-Halt vorhanden ist oder nicht, sind in jedem Fall an ausgewählten Stellen rund um die Maschine fix installierte, für jedermann erkenntliche und gut zugängliche Not-Halt Schalter anzubringen.

21.9 Bedienelemente zum Stillsetzen im Notfall

Die Maschinenrichtline stellt keine detaillierten Anforderungen zur Farbgebung der Bedienelemente zum Stillsetzen im Notfall. Die Anforderung lautet: "Die Befehlseinrichtung muss deutlich kenntliche, gut sichtbare und schnell zugängliche Stellteile haben".

Im Normalfall sind "Not-Halt" Schalter rot-gelb gekennzeichnet. Die besondere Gestaltung hat den Sinn einer Signalwirkung, und soll bewirken, dass jeder, speziell auch ungeschulte Personen, in einem Notfall, das Bedienelement rasch als die Einrichtung zur Beseitigung einer Gefahr erkennen kann.

Eine unbedingte Forderung ist daher, dass mit diesen derart gekennzeichneten Geräten, zu jeder Zeit und in jeder Betriebsart, ohne weitere Kenntnis über die Maschine, ein sicherer Zustand eingeleitet werden kann (siehe da-

© KEBA 2021

zu auch EN ISO 13850). Eine wechselnde Betriebsbereitschaft eines Not-Halt Schalters ist nicht zulässig, da dies in Paniksituationen zu Fehlhandlungen und lebensbedrohlichen Zeitverlusten führen kann.

Beleuchteter Not-Halt

Wireless Handbediengeräte sind für einen häufigen Betriebswechsel zwischen einer oder mehreren Maschinen vorgesehen und werden dort nur temporär, für Inbetriebnahme- oder Einrichtarbeiten benötigt.

Mit verschiedenen Maßnahmen, wie z.B. Basisstation CB4xx, werden die Not-Halt-Kreise der Maschine bei nicht verbundenem Handbediengerät überbrückt, sodass die Maschine im Normalbetrieb auch ohne Handbediengerät weiterlaufen kann. Start und Bedienung der Maschine können dann über eine unabhängige Bedieneinrichtung erfolgen.

Durch den häufigen Betriebswechsel der Handbediengeräte kann nicht ausgeschlossen werden, dass abgemeldete Handbediengeräte mit wirkungslosen Not-Halt zwischenzeitlich in der Nähe von in Betrieb befindlichen Maschinen liegen oder hängen und in Not-Situationen für funktionstüchtige Geräte gehalten werden.

Die Vorgangsweise, die konstruktive Beseitigung der Gefahr durch eindeutige Farbgebung, eventuellen organisatorischen Maßnahmen vorzuziehen, entspricht auch den bereits oben beschriebenen "Grundsätzen für die Integration der Sicherheit" der Maschinenrichtlinie und ist daher gesetzlich verpflichtend.

Aus diesem Grund dürfen funkbetriebene Handbediengeräte nur mit einem beleuchteten Not-Halt ausgestattet werden. Durch eine Veränderung der Farbe mittels Beleuchtung des aktiven Not-Halts wird eine Verwechslung zwischen Handbediengeräten mit aktivem und nicht aktivem Not-Halt vermieden.

Information

Wenn Not-Halt-Schalter auf kabellosen Bedienstationen (z.B. tragbaren Programmiergeräten) angebracht sind, dann muss immer mindestens ein Gerät mit (rot gelbem) Not-Halt verdrahtet (stationär) an der Maschine verfügbar sein!

21.10 Hinweise zum Zustimmtaster

Viele Maschinen verfügen über die Betriebsarten Normalbetrieb und Sonderbetrieb. Im Normal- (Automatik-) Betrieb erfüllt die Maschine ihren Einsatzauftrag. Die Sicherheit wird in dieser Betriebsart über geschlossene, trennende Schutzeinrichtungen und/oder mit funktionstüchtigen, nicht trennenden Schutzeinrichtungen gewährleistet. Die Sonderbetriebsarten einer Maschine dienen dazu, den Normalbetrieb aufrecht zu erhalten. Dabei muss die Sicherheit auf eine andere Art als im Normalbetrieb gewährleistet werden,

KEBA © KEBA 2021

da nun Gefahrenbereiche der Maschine betreten werden können, und gezielte Bewegungen möglich sein müssen. Hier spielt der Zustimmtaster eine tragende Rolle.

Voraussetzung für die Anwendung ist, dass mittels Zustimmtaster, die zu kontrollierende Gefährdung rechtzeitig ausgeschaltet werden, bevor ein Personenschaden auftritt. Hierfür sind eventuell zusätzliche Sicherheitsmaßnahmen, wie eine sicher reduzierte Geschwindigkeit von Antrieben notwendig.

Im Gegensatz zum Not-Halt (bzw. Stopp-) Schalter, befindet sich eine Maschine in den Sonderbetriebsarten mit Zustimmtaster immer im sicheren Zustand, solange dieser nicht betätigt ist - siehe Abbildung:

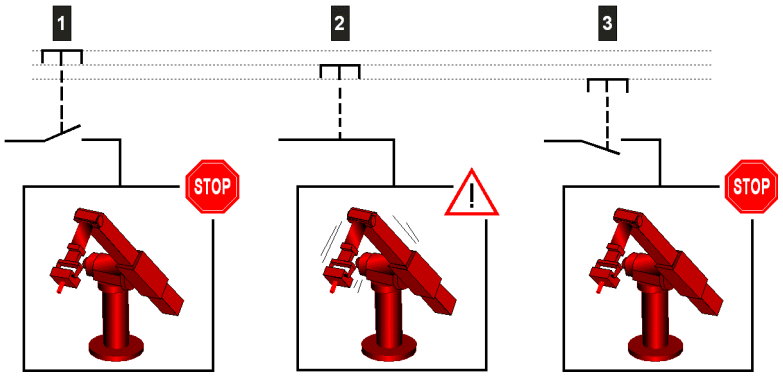


Abb. 21-113: Zustimmungsfunktionen

1 ... "Ruhestellung" (Zustimmtaster nicht betätigt)	2 ... "Zustimmung" (Zustimmtaster gedrückt)
3 ... "Panik" (Zustimmtaster stark gedrückt)	

Die Zustimmungs-Funktion ist auch in der EN 60204-1 beschrieben, und entspricht dem Stand der Technik.

Die Panikstellung bei 3-stufigen Zustimmtastern wurde deshalb eingeführt, da Menschen in Schrecksituationen häufig mit einer reflexartigen Verkrampfung der Gliedmaßen reagieren, und dann den Zustimmtaster nicht loslassen können. Deshalb führt das feste Durchdrücken des Zustimmtasters ebenfalls zur Ausschaltung.

Die Steuerung muss so ausgelegt werden, dass die Bewegung nicht direkt mit der Betätigung des Zustimmtasters eingeleitet wird, sondern erst durch die zusätzliche Betätigung einer Steuerungstaste. Dies können Folientasten am Handbediengerät sein, oder auch graphische Software-Tasten am Touchscreen.

Auch ein optional vorhandener Joystick kann zur Auslösung des Bewegungssignals verwendet werden.

Für die Zustimmungsfunktion sind lt. EN 60204 nur die Stopp-Kategorien 0 oder 1 erlaubt, d.h. mit dem Stoppen durch den Zustimmtaster muss in jedem Fall eine Energieabschaltung der Antriebe verbunden sein.

© KEBA 2021

Um eine missbräuchliche dauerhafte Betätigung des Zustimmtasters mittels mechanischer Fixiereinrichtungen zu verhindern, wird empfohlen, die maximale Dauer einer akzeptierten Zustimmung zu begrenzen. Dies muss durch eine dem Handbediengerät nachgeschaltete Steuerung realisiert werden.

Ein Zustimmtaster ist kein Ersatz für eine Zweihandschaltung, wie sie für manche Maschinen (z.B. Pressen) vorgeschrieben wird, und darf daher nicht damit verwechselt werden!

Im Gegensatz zum Zustimmtaster, zwingt die Zweihandschaltung während der Maschinenbewegung die gefährdeten Gliedmaßen des Bedienpersonals in eine sichere Position.

KEBA © KEBA 2021

22 Anhang: Chemikalienbeständigkeit

Die folgende Tabelle gibt einen Überblick über die grundsätzliche Chemikalienbeständigkeit der im T15xWL verwendeten Materialien. Die Liste hat keinen Anspruch auf Vollständigkeit.

Manche Substanzen haben starke Kriecheigenschaften, wodurch Substanzen schädlich ins Gerät und in Komponenten eindringen können. Diese Art der Beständigkeit wird hiermit nicht bewertet.

Die angegebenen Werte beziehen sich ausschließlich auf Labortests. Die eingesetzten Materialien unterliegen oftmals Einflüssen, die in Labortests nicht erkannt werden können (Temperatur, Druck, Luftfeuchtigkeit, etc.). Die angegebenen Werte dienen daher nur als Richtlinie. In Zweifelsfällen wird empfohlen einen Test durchzuführen.

In nachfolgender Tabelle werden die Materialien wie folgt abgekürzt:

G/S:	Gehäuse + Schachtdeckel
T:	Tastatur
AB:	Aufhängebügel
TS:	Touchscreen
H:	Handschlaufe
NH:	Not-Halt
ZT:	Zustimmtaster
USB:	USB
AK:	Anschlusskabel

Die Beständigkeit der Materialien wird in folgende Klassifizierungen unterteilt:

\+ Gute Beständigkeit o Bedingte Beständigkeit - Schlechte Beständigkeit

Medium	G/S	T	AB	TS	H	NH	ZT	USB	AK
Aceton CAS-Nr: 000067-64-1 Konzentration: -	o	+	+	+	+	+	+	o	+
Ammoniak CAS-Nr: 001336-21-6 Konzentration: 10%	+	+	+	+	+	+	+	+	+
Benzin CAS-Nr: 086290-81-5 Konzentration: -	+	+	+	+	+	+	+	+	+
Dieselkraftstoff CAS-Nr: - Konzentration: -	+	+	+	+	+	+	+	-	+
Essigsäure CAS-Nr: 000064-19-7 Konzentration: 10%	+	+	+	+	+	+	+	-	+
Ethanol CAS-Nr: 000064-17-5 Konzentration: 95%	+	+	+	+	+	+	+	+	+

© KEBA 2021

Medium	G/S	T	AB	TS	H	NH	ZT	USB	AK
Hydrauliköl (Mineralölbasis) CAS-Nr: - Konzentration: -	+	+	+	+	+	+	+	o	+
Kaliumhydroxid CAS-Nr: 001310-58-3 Konzentration: 10%	+	+	+	+	+	+	+	o	+
Leinöl CAS-Nr: 008001-26-1 Konzentration: -	+	o	+	+	+	+	o	o	+
Schneid-/ Schleiföl CAS-Nr: - Konzentration: -	+	o	+	+	+	+	o	o	+
Methanol CAS-Nr: 000067-56-1 Konzentration: -	+	+	+	+	+	+	+	+	+
Methylbenzol (Toluol) CAS-Nr: 000108-88-3 Konzentration: -	+	+	+	+	+	+	o	-	+
Methylethylketon (Butanon) CAS-Nr: 000078-93-3 Konzentration: -	o	o	o	+	+	+	o	-	o
Motoröl CAS-Nr: - Konzentration: -	+	o	+	+	+	+	+	o	+
Natriumhydroxid CAS-Nr: 001310-73-2 Konzentration: 10%	o	-	+	o	+	+	+	+	o
Petrolether (Leichtbenzin) CAS-Nr: 008032-32-4 Konzentration: -	+	+	+	+	+	+	+	+	+
Salzsäure CAS-Nr: 007647-01-0 Konzentration: 10%	+	+	+	+	+	-	+	-	o
Schmierfett CAS-Nr: - Konzentration: -	+	o	+	+	+	+	+	+	+
Schwefelsäure CAS-Nr: 007664-93-9 Konzentration: 10%	+	+	+	+	+	+	o	o	+
Silikonöl CAS-Nr: - Konzentration: -	+	+	+	+	+	+	+	+	+
Spiritus CAS-Nr: - Konzentration: -	+	+	+	+	+	+	+	o	+
Terpentin CAS-Nr: - Konzentration: -	+	+	+	+	+	+	+	-	+

KEBA © KEBA 2021

23 Anhang: Begriffe und Definitionen

Die Begriffe und Definitionen in diesem Dokument orientieren sich an der IEC 62443.

Anlageneigentümer

Ein Anlageneigentümer ist eine Einzelperson oder ein Unternehmen, das für ein IACS verantwortlich ist. Ein Anlageneigentümer kann für ein oder mehrere IACS verantwortlich sein.

"Boundary protection device"

Das Gerät, das die Netze auf sichere Weise verbindet, ist ein "Boundary protection device". Die Grenze ist die Kontaktzone dieser Netze. Das "Boundary protection device" ermöglicht die Partitionierung in separate Zonen. Diese getrennten Zonen sind Teil einer Strategie der Tiefenverteitigung ("Defense in Depth"). Sie sind auch für die Bedrohungs- und Risikobewertung eines Systems von Bedeutung.

IACS

IACS ist die Abkürzung für "Industrial Automation and Control System". Der Begriff IACS umfasst Systeme, die den sicheren und zuverlässigen Betrieb industrieller Prozesse beeinflussen oder beeinflussen. Er umfasst industrielle Steuerungssysteme wie SPS mit Kommunikationsnetzwerken, die im Mittelpunkt dieses Dokuments stehen.

Integrität

Integrität spiegelt die logische Korrektheit eines Systems, die logische Vollständigkeit von Hard- und Software und die Konsistenz von Daten wider.

Produktfamilie

Eine Gruppe von Produkten, die einen gemeinsamen Anwendungsbereich und verwandte Funktionen haben.

Verfügbarkeit

Die Wahrscheinlichkeit, dass ein Gegenstand zu einem bestimmten Zeitpunkt eine geforderte Funktion erfüllen wird. Es wird davon ausgegangen, dass die erforderliche Umgebung und die erforderlichen Ressourcen vorhanden sind.

Vertraulichkeit

Schutz vor der Weitergabe von Informationen an unbefugte Personen und Einrichtungen.

© KEBA 2021

Index

A
Abmessungen
Technische Daten 223
Allgemein
Technische Daten 217, 221
Anschlusserkennung
Verkabelung 102, 123, 141
Ausschalten 190

B
Battery-Pack 243
Box-ID
Adressschalter Position 147
Konfiguration 147

C
CNC-Tastatur 80

E
Ethernet
Allgemein 106, 125, 142
Pinbelegung 106, 125, 142
Status-LED Position 91
Verkabelung 106, 125, 142

F
Flash-Speichermedium 189
Folientastatur
CNC-Tastatur 80
Robotik-Tastatur 78
Standardtastatur 77
Freigabesteuerung
Normale Betätigung 88
Panik-Betätigung 88

G
Gewicht
Technische Daten 223

H
Herunterfahren 190

K
Kabelauslässe
Position 92
Technische Daten 100, 121, 139
Key-Mapping 183
Konfiguration
Gerätekonfiguration 150

L
Leuchtdrucktaster
Position 91

M
Mechanische Eigenschaften
Technische Daten 220
Micro SD-Schnittstelle
Technische Daten 223

N
Not-Halt
Position 91
Verkabelung 101
Not-Halt Konfiguration
LED Position 91
Not-Halt-Funktion
Technische Daten 226
Verkabelung 101

KEBA © KEBA 2021

P

Power-LED
Position ... 91
Power-Taste ... 190
Prozessor ... 221
PS/2 Code ... 183

R

RFID
Technische Daten ... 222
Robotik-Tastatur ... 78

S

Schlüsselschalter
Verkabelung ... 102, 123, 141
Schnittstellen
Technische Daten ... 222, 223, 224
Schutzhülle
Bestellnummer ... 237
Signalsäule
Verkabelung ... 103, 124, 141
Spannungsversorgung
Technische Daten ... 223
Verkabelung ... 101, 122, 140
Standardtastatur ... 77
Status-LED-Balken
Allgemein ... 95, 116, 134
Betriebszustände ... 190
Fehlerzustände ... 201
Position ... 91

T

Tastatur
CNC-Tastatur ... 80
Robotik-Tastatur ... 78
Standardtastatur ... 77
Tastenmanagement ... 183
Trageset
Bestellnummer ... 238
Typenschild
Position ... 93

U

Umgebungsbedingungen
Technische Daten ... 217, 235, 236
USB-Schnittstelle
Technische Daten ... 222

V

Versorgung
Technische Daten ... 221

Z

Zusatz-Akku ... 243
Bestellnummer ... 244
Lagerung ... 245
Lebensdauer ... 245
Zubehör ... 244
Zustimmtaster
Technische Daten ... 225

© KEBA 2021

© KEBA 2021