KeTop

KeTop T15xWL / CB4xx
Safe Wireless System (T15xWL / CB4xx)
Project engineering manual V 1.07

Translation of the original manual

KEBA
Automation by innovation.

Document: V 1.07
Pages: 260

© KEBA 2021
Specifications are subject to change due to further technical developments. Details presented may be subject to correction.

All rights reserved.

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

For information about KEBA and our subsidiaries please look at www.keba.com.

Record of Revision

Version	Date	Change in chapter	Description	Changed by
1.00	07-2021	-	Newly created	hasl
1.01	10-2021	Various chapters	Change to new corporate structure, UKCA, standards restructured	hasl
1.02	03-2023	Various chapters, device configuration, Profinet configuration, connection log, cleaning the touchscreen, robotics keypad, directives, standards and regulations	New CB4xx variants added, operation area monitoring expanded, various updates, new keyboards added, revision of the standards	hasl, rmr
1.03	05-2023	Safety notes, operation area monitoring, front view of handheld devices, displays and operating elements, CB41x base station, CB42x base station, configuration, validation, connection to the base station, safety parameters, accessories, declaration of conformity	Various changes and additions	rmr
1.04	11-2024	Power supply, mounting and installation instructions, base station CB 42x,process data image, configure hibernation, operation and handling, technical data base station, battery, standards for the American market, configuration, type plate, accessories	Content removed from chapter, updated positioning of the base station, updated images, adapted connection and wiring, updated data, various changes, operating state added, inrush current added, content and technical data extended, UL 1740 removed, interrupt AutoLogon added, base station CB 43x added, UKCA removed, battery pack added	ext_klapper
1.05	03-2025	Maintenance, Options	Backup with BSS adapted, added order numbers	ext_klapper
1.06	07-2025	Windows settings, Configuration	EtherCAT updated, intended use updated, ePKEA added, information about display brightness >70 % added	ext_klapper

© KEBA 2021

1.07	04-2026	Displays and Controls, Accessories, Various chapters	Added CNC keyboard and carrying strap for protective cover, Updated EU Battery Directive, OAM, DIP switches, new battery, protective foils, Intel Atom x6211, order overview, and error states, updated nameplate, WEEE and disposal labeling, and battery information	ext_klapper, bebe

KEBA © KEBA 2021

Table of contents

1 Introduction ... 13
- 1.1 Purpose of the document ... 13
- 1.2 Preconditions ... 13
- 1.3 Intended use ... 14
  - 1.3.1 Products ... 15
  - 1.3.2 Cybersecurity ... 16
  - 1.3.3 Defense in Depth ... 36
  - 1.3.4 Protected environment ... 37
  - 1.3.5 Network architecture ... 38
  - 1.3.6 Network properties ... 43
  - 1.3.7 Remote access ... 44
  - 1.3.8 Reference IACS ... 45
- 1.4 Notes on this document ... 47
  - 1.4.1 Contents of document ... 47
  - 1.4.2 Not contained in this document ... 48
- 1.5 Documentation for further reading ... 48
- 1.6 Conformity of safety fieldbusses ... 48
  - 1.6.1 EtherCAT declaration ... 48
  - 1.6.2 PROFINet / PROFIsafe declaration ... 49
- 1.7 Information in relation to MRL 2006/42/EC ... 49
  - 1.7.1 Quantitative safety relevant specifications for emergency stop-button and enabling device ... 49
  - 1.7.2 Relationship between Performance Level and Safety Integrity Level 49
  - 1.7.3 Abbreviations ... 50
- 1.8 Emergency stop switch ... 50

2 Safety notes ... 52
- 2.1 Representation ... 52
- 2.2 General safety instructions ... 53
- 2.3 Personnel safety instructions ... 55
- 2.4 ESD information ... 58

3 System overview ... 59
- 3.1 Operation area monitoring (= OAM; optional) ... 60
- 3.2 Order overview ... 64

4 Description of the handheld devices ... 67
- 4.1 Front view ... 67

© KEBA 2021

4.2 Rear view ... 68
4.3 Handling ... 68
4.4 Type plate ... 69
4.4.1 Type plate Celeron N2807 ... 69
4.4.2 Type plate Intel Atom x6211 ... 70
4.5 Display and operating elements ... 71
4.5.1 Standard keypad ... 71
4.5.2 Robotics keypad ... 72
4.5.3 CNC keypad ... 73
4.5.4 Status LEDs ... 74
4.5.5 "Ident" button ... 75
4.5.6 Touchscreen ... 75
4.6 Connection and wiring ... 76
4.6.1 Cable entrance area ... 76
4.6.2 Plugging in battery ... 76
4.6.3 Power supply ... 77
4.6.4 Illuminated emergency stop ... 77
4.6.5 Enabling switch ... 79
4.6.6 USB port ... 82

5 CB41x base station ... 83
5.1 Front view ... 83
5.2 Rear view ... 84
5.3 Bottom view ... 84
5.4 Top view ... 85
5.5 Type plate ... 85
5.6 Displays and operating elements ... 85
5.6.1 Status LEDs ... 85
5.6.2 Connection LEDs ... 86
5.6.3 Status LED bar ... 86
5.6.4 "Pairing Reset" button ... 87
5.7 Mounting and installation instructions ... 87
5.7.1 Positioning the base station ... 88
5.7.2 Drilling template for wall mounting ... 88
5.7.3 Installing the base station ... 89
5.8 Connections and wiring ... 90
5.8.1 Terminal strip S1 / Power supply ... 93
5.8.2 Terminal strip S2 ... 94
5.8.3 "Signal" terminal strip ... 95
5.8.4 "Pairing" / "Remote Pairing" outputs terminal strip ... 95
5.8.5 Terminal strips for fast response buttons ... 96
5.8.6 Ethernet ... 97

KEBA © KEBA 2021

5.8.7 Changes to the wiring ... 98
5.8.8 Closing the base station ... 99
5.8.9 Emergency stop ... 99
5.8.10 Connection example of the enabling function with monitoring device (PILZ PNOZ s3) ... 100
5.8.11 Connection example for enabling function and emergency stop with KEBA safety control ... 101

6 Base station CB42x ... 103
6.1 Front view ... 103
6.2 Rear view ... 104
6.3 Bottom view ... 104
6.4 Top view ... 105
6.5 Type plate ... 105
6.6 Displays and operating elements ... 105
6.6.1 Status LEDs ... 106
6.6.2 Connection LEDs ... 106
6.6.3 Status LED bar ... 107
6.6.4 "Pairing Reset" button ... 107
6.7 Mounting and installation instructions ... 108
6.7.1 Positioning the base station ... 108
6.7.2 Drilling template for wall mounting ... 109
6.7.3 Installing the base station ... 109
6.8 Connections and wiring ... 110
6.8.1 Internal wiring ... 113
6.8.2 Terminal strip S1 / power supply ... 113
6.8.3 Terminal strip S2 ... 114
6.8.4 "Signal" terminal strip ... 114
6.8.5 Ethernet ... 115
6.8.6 PROFINET ... 116
6.8.7 Changes to the wiring ... 117
6.8.8 Closing the base station ... 117
6.8.9 Emergency stop ... 118
6.9 Error acknowledgement ... 118

7 Base station CB43x ... 120
7.1 Front view ... 120
7.2 Rear view ... 121
7.3 Bottom view ... 121
7.4 Top view ... 122
7.5 Type plate ... 122
7.6 Displays and operating elements ... 122
7.6.1 Status LEDs ... 123

© KEBA 2021

7.6.2 Connection LEDs ... 123
7.6.3 Status LED bar ... 124
7.6.4 "Pairing Reset" button ... 125
7.7 Mounting and installation instructions ... 125
7.7.1 Positioning the base station ... 125
7.7.2 Drilling template for wall mounting ... 126
7.7.3 Installing the base station ... 127
7.8 Connections and wiring ... 128
7.8.1 Internal wiring ... 130
7.8.2 Terminal strip S1 / power supply ... 131
7.8.3 Terminal strip S2 ... 131
7.8.4 "Signal" terminal strip ... 132
7.8.5 Ethernet ... 133
7.8.6 EtherCAT ... 133
7.8.7 Changes to the wiring ... 134
7.8.8 Closing the base station ... 134
7.8.9 Emergency stop ... 135
7.9 Error acknowledgement ... 136

8 Configuration ... 137
8.1 Box ID configuration ... 137
8.2 F addressing (only for CB42x and CB43x) ... 138
8.3 Operation area configuration (safety-related) ... 139
8.4 Device configuration (Device Config) ... 140
8.4.1 Base station ... 141
8.4.2 Diagnosis data ... 145
8.4.3 Display ... 146
8.4.4 Licenses ... 147
8.4.5 Network ... 147
8.4.6 Reboot ... 152
8.4.7 Shutdown ... 152
8.4.8 Version info ... 153
8.5 PROFINET configuration (only for CB42x) ... 153
8.5.1 Process data image ... 154
8.6 EtherCAT / FSoE configuration (only for CB43x) ... 157
8.6.1 Process data image ... 157
8.7 Configure hibernation ... 159
8.8 Remote access to KeTop ... 160
8.8.1 Remote Access via OpenSSH ... 161
8.9 Security settings ... 162
8.9.1 (Un-) installation ... 162
8.9.2 Whitelisting using AppLocker ... 163

KEBA © KEBA 2021

8.9.3 Kiosk Desktop ... 163
8.9.4 KEBA Write Filter ... 168
8.10 Connectivity protocols ... 169
8.11 Key management ... 171
8.11.1 Key codes ... 172
8.12 Windows settings ... 173
8.13 Programming ... 175

9 Operation and handling ... 176
9.1 Start-up ... 176
9.2 Shut down the KeTop ... 176
9.3 Base station operating states ... 177
9.4 Operating behavior ... 178
9.5 Charging behavior of the battery ... 179
9.6 "System State" Dialog ... 180

10 Validation ... 181
10.1 Validating the distance measurement ... 181

11 Pairing to base station ... 182

12 Diagnosis ... 188

13 Maintenance ... 190
13.1 Cleaning the touchscreen ... 190
13.2 Changing the battery ... 190
13.3 Creating a service medium ... 191
13.4 Creating a backup ... 192
13.5 Restoring a backup / Performing an update ... 193
13.6 Replacing the storage medium ... 194

14 Disposal ... 196
14.1 Disposal of the module ... 196
14.2 Disposal of the battery ... 196

15 Technical data ... 198
15.1 General ... 198
15.2 Environmental conditions ... 198
15.3 Safety characteristics ... 198
15.3.1 System response time with safe fieldbus connection (for CB42x and CB43x) ... 200
15.4 Mechanical properties ... 201
15.5 Battery / Rechargeable Battery ... 201

© KEBA 2021

15.6 Technical data handheld device 202
15.6.1 General 202
15.6.2 Power supply 202
15.6.3 Processor 202
15.6.4 Interfaces 203
15.6.5 Dimensions, weight 204
15.7 Technical data base station 204
15.7.1 Power supply 204
15.7.2 Interfaces 204
15.7.3 Terminal strips 205
15.7.4 Enabling function 206
15.7.5 Emergency stop function 207
15.7.6 Dimensions, weight 207

16 Optional operating elements 209
16.1 Rotary Encoder Switch with 16 positions 209
16.2 Key-operated switch 209
16.3 Illuminated push button 209
16.4 Handwheel 210
16.5 Digital joystick 210
16.6 Camera 211

17 Accessories 212
17.1 KeTop CS 15x charging station 212
17.2 Power supply unit 213
17.3 Battery 214
17.3.1 Battery Celeron N2807 215
17.3.2 Rechargeable Battery Atom x6211 216
17.4 Bumper / carrying set 217
17.4.1 Attaching the bumper 219
17.4.2 Cleaning 220
17.4.3 Storage and transportation 221
17.5 Handle and hand strap 221
17.5.1 Assembly 221
17.6 Battery pack 223
17.6.1 Using the battery pack 226
17.6.2 Charging the battery pack 227
17.6.3 Technical data 228
17.7 Rear wall for cable installation on the back side (only for CB41x) 229
17.8 Tempered Glass Screen Protector 230

18 Directives, standards and regulations 231
18.1 EU directives / Regulations 231

KEBA © KEBA 2021

18.2 Standards for checking the conformity ... 231
18.3 Other standards ... 232
18.4 Regulations ... 235
18.5 Standards for the American market ... 235
18.6 Standards for the Canadian market ... 236
18.7 Standards for the Japanese market ... 236

19 EU Declaration of conformity ... 241

20 Appendix: Commissioning ... 244

21 Appendix: Machinery safety ... 245
21.1 Hazard and risk analysis ... 246
21.2 Principles for the integration of KeTop ... 246
21.3 Technical construction file ... 247
21.4 State of the art ... 248
21.5 Recognition of conformity by means of harmonized standards ... 248
21.6 Selection of Performance Level and Safety Categories in accordance with EN ISO 13849-1 ... 248
21.7 Application of handheld terminals in special operating modes ... 250
21.8 Information about the emergency stop button ... 250
21.9 Manual control of machines in special operating modes ... 251
21.10 Information about enabling switches ... 252

22 Appendix: Chemical resistance ... 255

23 Appendix: Terms and definitions ... 257

Index ... 258

© KEBA 2021

KEBA © KEBA 2021

1 Introduction

1.1 Purpose of the document

This document describes the Safe Wireless system. The system consists of a battery-powered mobile handheld device and a permanently installed base station. The handheld device has the emergency stop safety function and enabling switch, which are wirelessly connected to the base station.

This document contains all of the relevant requirements from the Machinery Directive 2006/42/EC (for a description of the machine, see Chapters 3-5).

Information

The manual is written exclusively for the target groups listed in this manual. The machine manufacturer or system supplier must incorporate the safety information required for end customers into the operating manual for end customers in the applicable national language.

1.2 Preconditions

This document contains information for persons who meet the following requirements:

Target group	Required knowledge and abilities
Safety engineer for "Functional Safety"	Technical basic education (advanced technical education, engineering degree or corresponding professional experience) Knowledge about: ● Principles of functional safety ● All relevant standards and safety regulations for the machine/system, especially knowledge of validation in acc. with EN ISO 13849-2 ● Special risk potential of the machine/system and the production process ● Specific protective measures to avert machine-specific hazards (based on hazard and risk analysis) ● Functioning and application limits of the safety components (including safety PLC). ● In-depth knowledge of national accident prevention regulations
Project engineer	Technical basic education (advanced technical education, engineering degree or corresponding professional experience). Knowledge about: ● Currently valid safety regulations ● The method of operation of a PLC ● The application

© KEBA 2021

Target group	Required knowledge and abilities
Electrician	Technical training in electrical engineering (based on industry-standard training guidelines). Knowledge about: ● Currently valid safety regulations ● Wiring guidelines ● Circuit diagrams ● Professional manufacture of electrical connections in conformity with national and international regulations
Start-up technician	Technical basic education (advanced technical education, engineering degree or corresponding professional experience). Knowledge about: ● Currently valid safety regulations ● Method of operation of the machine or system ● Fundamental functions of the application ● System analysis and debugging ● Setting options on the operating devices
Service technician	Technical basic education (advanced technical education, engineering degree or corresponding professional experience). Knowledge about: ● The method of operation of a PLC ● Currently valid safety regulations ● Method of operation of the machine or system ● Diagnostic options ● Systematic fault analysis and troubleshooting

1.3 Intended use

The intended use of the handheld devices ranges from monitoring and parameterization to the operation of machines, such as:

- Injection molding machines
- Robots
- Textile machines
- Printing machines

in the normal operating modes, such as

- Automatic

as well as in semi-automatic or manual special modes, such as

- Setup
- Teach
- Test run

The available safety functions include an enabling switch and an illuminated emergency stop.

KEBA © KEBA 2021

The emergency stop and enabling switch are dual-circuited and allow the implementation of Category 4 PL e according to EN ISO 13849-1 taking into account the operating cycles with regard to the B_{10D} values of the safety components.

The machine manufacturer is responsible for selecting a handheld terminal that is suitable for the machine and designing any possible additional options that must be implemented in accordance with the legally required hazard and risk evaluation.

Please also observe the appendices relating to the intended use of the handheld terminal.

KEBA products as KeTop, KeControl, KeConnect and KeDrive are components for industrial automation and control systems (IACS). An IACS can be used to operate a variety of systems. It can be used to control individual machines (such as injection molding machines), but also to operate larger systems (such as entire plants).

KEBA products can be used for any type of machine or system if the product meets the necessary requirements and corresponds to the intended use of the product. They are designed as IACS components with a focus on machine builders and can also be used in factory automation systems that control multiple machines.

1.3.1 Products

The KEBA products for IACS are grouped into the following product families:

- KeTop
  - Handheld terminals
  - Operating panels
- KeControl
  - Controls
  - Industrial PCs
  - Robot controllers
- KeConnect
  - Digital input/output
  - Analog input/output
  - Temperature input
  - PWM output
  - Encoder interfaces
  - RS232, RS422, RS485 interfaces
  - IO-Link interfaces
  - …
- KeDrive
  - Servo controllers
- KeStudio
  - Software toolsKeTop-, KeControl-, KeConnect- and KeDrive-products

© KEBA 2021

Every product family contains a wide range of products. They contain physical products like a PLC device or a digital output device. They also contain software which is necessary to operate those devices. This software can be software, which runs on the devices, and also software, which is used to communicate with the devices.

1.3.2 Cybersecurity

KEBA IACS components follow a common set of safety principles. These security principles enable the owner of the system to achieve a high level of security. They also provide an understanding of how security is designed and how it works in practice. First, the general security principles for all KEBA IACS components are presented. The specific security principles of devices for automation networks and devices for machine networks are then described. The remaining chapters focus on the security of software services and functions of KEBA IACS components.

The owner of the system determines the required safety level. If the required safety level is low, certain safety principles can be omitted. Therefore, the system owner decides which security principles are actually implemented and present. The configuration of the KEBA IACS components allows security features to be deactivated.

Each KEBA IACS component has individual functionalities to meet the requirements of machine builders and system integrators. The list of software services and functions supported by KEBA-IACS components therefore depends on the specific product. The software services and features actually supported are documented in the product-specific documentation. This document refers to product families to provide an overview of the supported software services and features.

Information

Not all KEBA devices with Windows as the operating system support the features in exactly the same way, but the principles are just as valid and must be implemented in part with standard Windows functions (e.g. user administration, ...).

1.3.2.1 Cybersecurity objectives

Cybersecurity focuses on the following objectives, which apply to IACS in the following order:

1) Availability
2) Integrity
3) Confidentiality

Availability usually has the highest priority, as a production stop can lead to considerable financial losses. Integrity often comes second, as the controlled processes and machines may only be operated as intended within known limits in order to meet quality requirements. IACS do not use or protect trade secrets such as financial data. Unlike IT systems, confidentiality is therefore generally less important for IACS than availability and integrity.

KEBA © KEBA 2021

1.3.2.2 General security principles

The following general security principles are valid for all KEBA IACS components.

Authentication

Authentication is a prerequisite for any access to an IACS component. No matter if information is read or if actions are executed, a successful authentication is necessary first. Multiple mechanisms exist which allow a secure authentication:

- **Password**: Passwords are still used for authentication. If passwords are used, then it should be taken care that the passwords provide a sufficient security level against threats like dictionary attacks or brute force attacks. Passwords are used by e.g. web interface and DevAdmin.
- **Key**: Asymmetric cryptographic keys are state of the art for authentication. Such keys are used by e.g. SSH.
- **Certificate**: Certificates are public keys, which are signed by a certificate authority (CA). For authentication, the ownership of the private key is challenged and the signature of the CA is validated. Certificates are used by e.g. DevAdmin, OPC UA, and OpenVPN.
- **Geographical location**: The location can be used for authentication if physical access restrictions exist for that location. This is the case for shop floors which can only be entered with a valid key card or for a cabinet which can only be opened with a unique key. Furthermore, a device that is designed to provide functions to physically present persons can also use the location as authentication. Geographical location is used for authentication by e.g. display and operating elements of , , and devices.
- **Key card**: Key cards are a wide spread mechanism for authentication. A secret is stored on the key card. This secret is used for the authentication. Key cards are used by e.g. visualization on devices.

Secrets used for authentication must be strong enough to fulfill the security level required by the asset owner. They shall not be guessable. Policies help to ensure that passwords and keys are strong enough and are protected against becoming public. The authentication management is done with dedicated interfaces and tools. For KEBA devices and DevAdmin are available for user and authentication management.

No default logins

Default passwords are a common attack vector. Even a strong default password does not increase the security level, because every default password is known by a broad group of people. Same is true for default private keys. Therefore, KEBA IACS components do not provide any default passwords or private keys. All passwords and the corresponding public keys of private keys must be set during setup or later. If no password or public key is set, then authentication for corresponding service is not possible and the service cannot be used.

© KEBA 2021

Encryption

After successful authentication, data can be transferred. This data is at risk of eavesdropping and manipulation. Therefore, encryption is used to ensure confidentiality and integrity of the transferred data. The used protocols shall support state of the art encryption algorithms. Encrypted communication is provided by protocols like e.g. HTTPS, SSH, OPC UA, and OpenVPN.

Least privilege

Successful authentication shall enable access to a minimal set of information and actions. The limitations can be defined by the service, which is accessed, and/or by the user, who is authenticated. This principle of least privilege lowers the risk of serious security bugs as the attack surface is reduced significantly. Additionally, it limits the gain of access rights if an attacker has overcome the authentication. This provides security advantages in particular if during operation only the minimum set of privileges is in use and available.

Limitations based on the authenticated user are available for e.g. visualizations and SSH. For visualizations functions and masks can be restricted to certain users. For SSH shell access and file access can be restricted based on the user.

Examples for limitations based on the service are OpenVPN and displays with operating elements. All provide a defined set of information and actions which fit to a secure use during operation.

Physical access restriction

An IACS cannot be operated securely if physical access is possible for anyone. With physical access e.g. cables can be manipulated or swapped. This will violate the security objectives availability and integrity, without any digital interaction. Therefore, it is a prerequisite that KEBA IACS components are protected by physical access control. Access restrictions are necessary for the shop floor and for the cabinet. Usually access to the cabinet is allowed to a smaller group than access to the shop floor. So access to the shop floor does not automatically include access to the cabinet.

Physical access control can be established with simple measures like keys or key card. This is usually sufficient for employees. For external guests or technicians even more elaborate measures like security gates with dedicated security guards are possible.

1.3.2.3 Automation network devices

The KEBA product families and are designed to be used in automation networks. These IACS components are able to fulfill the general security principles listed above. As a prerequisite, the integrated firewall of these devices must be configured to allow only secure services. The following secure services are in use:

- HTTPS (web interface)
- OPC UA
- SSH

KEBA © KEBA 2021

- OpenVPN

Depending on the requirements of the asset owner, the firewall can be configured to be more permissive and allow all active services, regardless whether they are secure or not. This of course reduces the security level of the automation network. Further threat and risk assessment executed by the asset owner is required to ensure that even with these services without authentication and encryption the required security level is reached.

and devices can also be used as boundary protection devices between the automation network and the machine network. The firewall of these devices handles traffic in a network specific way. The traffic from the automation network is restricted and can access only selected services; e.g., secure services like HTTPS. On the other side, traffic from the machine network is not restricted and can access all services. Furthermore, routing between the two networks is disabled. Thus, this boundary protection devices ensure segmentation of the automation network and the machine network.

KeControl product family

Products of the family are devices which are able to run customer applications to control machines and processes. They are equipped with powerful CPUs and run Linux as operating system. KEBA software is installed on these devices and enables customer s to write applications with a rich set of physical and logical interfaces. The installed KEBA software and the customer application determine if the product is used as PLC, robot controllers, or just as IPC.

KeTop product family

Products of the family are devices which provide user interfaces like displays and operating elements to enable the interaction of humans with machines and systems. The product family has various subfamilies with significant differences from the security point of view:

- **Active operating panel**: They provide a display with touch and additional operating elements and are additionally equipped with powerful CPUs, which run an operating system. The GUI application runs directly on the CPU of the active panel. An active panel can be used as automation network device and boundary protection device. The operating system is Linux or Windows.
- **Passive operating panel**: They act as monitor and provide a display with touch and additional operating elements. The GUI application runs on a separate device and the passive operating panel is connected to this device. A passive operating panel cannot be used as automation network device, because it has no network interfaces and it is just an accessory for devices .

1.3.2.4 Machine network devices

The KEBA product families and are designed to be used only as machine network devices. Machine network devices are not able to fulfill the general security principles from above completely. For field bus communication authentication and encryption is usually not available. Thus, physical access

© KEBA 2021

protection and least privilege are the only security principles that can be required for machine network devices. and devices fulfill both security principles. and devices fulfill these security principles as well, but can also be used as automation network devices.

The physical access protection to the cabinet, which contains the machine network, enables geographical location as authentication for all machine network devices. A technician, who can open the cabinet, is allowed to manipulate the whole software and hardware of the cabinet. Both, software and hardware, follow the least privilege principle to allow access to a defined set of information and actions.

The following secure services are in use for KEBA machine network devices:

- HTTPS (web interface)
- OPC UA
- SSH (including SFTP)

In addition to the secure services the following services and protocols without authentication and encryption are in use for KEBA machine network devices:

- Field buses (EtherCAT, PROFINET, CANopen, EtherNet/IP, …)
- RPC based services
- KVC
- EtherCAT mailbox gateway
- PLC protocols for non-KEBA PLCs (ADS, S7, Modbus)

KeConnect product family

Products of the family are devices with various types of inputs, outputs and interfaces for the automation of machines and processes. They can be attached directly to the PLC or can be connected to the PLC over a field bus for decentralized use. devices do not cross boundaries to other security relevant zones. All inputs, outputs, interfaces and the communication with the PLC are limited to the machine and the machine network. Even digital interfaces for encoders or IO-Link are designed only for local communication. Therefore, the machine and the machine network provide a protected environment for the operation of devices.

The latest devices use the EtherCAT field bus as communication interface. This field bus combines high performance with low implementation effort for the devices. Security in the form of authentication and encryption is not the focus of this and any other field bus. The security relies on the geographical location of the devices and physical access control. This enables economic implementation of automation solutions with high performance.

KeDrive product family

Products of the family are devices with various types of interfaces to control motors for the automation of machines and processes. They are usually connected to the PLC over a field bus. Some variants can be attached directly to

KEBA © KEBA 2021

the PLC. devices do not cross boundaries to other security relevant zones. All inputs, output, interfaces and the communication with the PLC are limited to the machine and the machine network. Even digital interfaces for encoders are designed only for local communication. Therefore, the machine and the machine network provide a protected environment for the operation of devices.

devices use field buses as communication interface. These field buses combine high performance with low implementation effort for the devices. Security in the form of authentication and encryption is not the focus of the field buses. The security relies on the geographical location of the devices and physical access control. This enables economic implementation of automation solutions with high performance.

The DriveManager software tool is used to configure and diagnose products. The tool communicates with the device over an IP based protocol. The used communication protocol does not support authentication or encryption. Therefore, this communication shall be limited to the machine network. The direct use of the DriveManager communication within the automation network or any other network without any additional security measures is strongly discouraged. Secure tunnels like OpenVPN can be used to allow DriveManager access within other networks than the machine network in a secure way.

device support passwords to limit the access to certain parameters. These passwords are only used to provide different filters for the list of available parameters. The parameters access itself is not protected by these passwords. Thus, the passwords of devices are no security relevant functionality. The security of devices does not rely on these passwords.

1.3.2.5 Authentication management

Authentication is the base for most secure services. The communication partners authenticate each other in a secure way before the actual encrypted communication starts. Also local access to privileged actions and information is protected by authentication.

The authentication shall always limit the access following the principle of least privilege; e.g., only a user with the role “Setup” has the rights to modify certain settings. User active during normal operation shall be restricted to the necessary minimum of privileges to limit the effects of possible security incidents.

and devices support the KEBA authentication management. User interfaces for authentication management, which provide a good overview and are easy to use, prevent mistakes with serious security consequences. K and DevAdmin are the interfaces for the authentication management of these devices.

The use of the authentication management of the operating system is also possible for selected products. This chapter is only about the KEBA authentication management. The operating system specific authentication management is documented in the user manuals of the operating system.

© KEBA 2021

Authentication management includes the management of user accounts and the assigned identifiers and authenticators. But authentication is not only about users. Authentication also includes the management of keys and certificates specific to services.

User management

With the KEBA user management, users can be created, configured and deleted. Additionally, roles can be created, configured and deleted. These roles can be assigned to users. A single user can have multiple roles assigned. Users with roles can authenticate, but are still not allowed to do anything if no rights are assigned to these roles. These rights are predefined and cannot be created or deleted. They are used by the software to decide whether access is granted or not. A single role can have multiple rights assigned. Furthermore, user settings and meta data can be configured.

Every user needs a unique identifier. For the KEBA user management the unique identifier is the username. There is no additional ID assigned to the user. Passwords are used as authenticator for all users.

For KEBA devices there is one default user named “Administrator” which is assigned to the default role “Administrator”. The user “Administrator” can be renamed, but the role “Administrator” not. The default role “Administrator” has all rights assigned. Thus, access to the user management itself is always granted for this role. Therefore, the user with this role is the key to the whole device. The password for at least one user with the role “Administrator” should be set, otherwise no user access can be enabled afterwards and access originating in the automation network is not possible. There is no default password. Further default users that can exist are “Operator”, “Service”, and “Teacher”.

Default roles

Roles require rights to actually enable access. Rights are fine-grained to enable a precise assignment of the minimum privileges to roles and users. To help users with the selection of rights, predefined default roles are available. These default roles have a proper set of rights assigned, which matches to the task of the role. Usually users can be modelled solely with these default roles. The list of default roles is kept short to facilitate easy understanding and use of the roles. The available default roles are:

- **Configuration**: This role allows access to all configurations, which are necessary to integrate the device into an environment. These configurations have to follow the requirements of the environment and cannot be set arbitrary without any consequences. This role allows the basic configuration of a machine, which does not require machine specific know how. It does not include application or machine specific configurations. Examples are settings related to the automation network like the automation network IP address and time server configuration.
- **Setup**: The setup role allows more extensive configurations than the configure role. It allows everything not covered by the configure role except user management. The setup role allows access to application/machine-specific settings. Also, software installation, updates, and backups

KEBA © KEBA 2021

are allowed and the application can be changed. Configurations related to the machine network are application/machine specific and therefore covered by this role. Other examples are firewall configuration and firmware update.

- **Access**: The access role allows the management of users and roles and the assignment of rights to roles. If a user has this role, then it effectively has all rights, because it can assign all rights to itself. Thus, this is a special role, which is assigned to only a few, ideally only one, user.
- **Application**: This role allows access to all variables and actions needed during operation. Ideally only this role is assigned to users to follow the principle of least privilege. As users with this role can be active permanently, it reduces the security risk if no other roles and rights are also potentially available permanently. Examples where this role should be used are SCADA systems or other devices which communicate over web interfaces during operation.
- **Development**: Access to everything needed for application development is allowed with this role. Application download, execution, and debugging is included. All types of applications like IEC, XCRT, and Visualizations are allowed.
- **Diagnosis**: The diagnosis role shall enable easy access to diagnosis data. This role does not allow any modifications and can be assigned safely to broad range of users. With the diagnosis role software versions and type labels can be read, the configured and available devices can be listed, the PLC trace can be read, status reports can be triggered and copied, and various other information can be accessed.
- **Visualisation**: This role enables access to visualizations over network. The functionalities provided by a visualization can be very broad and depend on the actual application. Therefore, generic roles do not fit and this specific role is used.

The list above only provides an overview what can be done with a certain role and its assigned rights. The exact required rights for certain information, actions and interfaces are documented in the user manuals.

Key and certificate management

Authentication is not only about users and passwords. Keys are also in use; e.g., for SSH user authentication. Additionally, certificates are often used for mutual authentication of services. Certificates contain public keys and are signed with private keys. Keys and certificates need to be generated. Their format and properties are specific to the services for which they are used. This renders the manual generation of keys and certificates a difficult task with various potential mistakes. Therefore, the KEBA authentication management supports the generation of keys and certificates. Some keys and certificates are generated during the first boot of a device. Other keys and certificates are generated on demand within the user interface DevAdmin. For selected services installation instead of generation is possible for keys and certificates.

© KEBA 2021

Public keys and certificates can be pre-installed. This is necessary for authentication and verification of data. This is no security risk as public keys and signatures are no secrets, which must be kept confidential. On the other hand, private keys are secrets. Thus, private keys are never pre-installed and no default private keys are used.

1.3.2.6 Automation network services

KEBA IACS components are able to provide various services to the automation network with specific security properties. These specific security properties need to be known to decide if a service should be used and how it is configured to provide the required security level. The product documentation will indicate whether a particular service is supported or not.

Web interface

The web interface provides an extensive collection of RESTful and WebSocket (WS) APIs for nearly all features related to KEBA IACS components. and devices support the web interface. Examples for APIs are:

- Variable service
- Device service
- File service
- Access service
- Configuration
- …

HTTPS is the secure protocol used for the web interface. HTTP is also supported, but should be restricted to the machine network and needs to be enabled explicitly. If needed, the firewall enables the restriction of HTTP to the machine network for boundary protection devices if HTTP cannot be eliminated.

Authentication is required for any use of the web interface. The authentication is based on the KEBA user management. Depending on the rights assigned to roles of users, access to APIs is allowed or not. Especially the access to the access service API for authentication management shall be allowed only for a minimal set of roles and users, because authentication settings and passwords can be changed with this API. Users with the role “Administrator” have access to the complete web interface including the access service API. Users without any rights relevant to the web interface have no access to the web interface.

If no certificate is configured during target setup in , then a certificate is generated at the first boot. This certificate is self-signed and expires after 90 days. The check for signed and not expired certificates needs to be deactivated in the HTTPS client if this generated certificate is used. This generated certificate provides a lower security level than a signed certificate, which is exchanged regularly before expiration. The authentication of the server is weaker, but encryption of the communication is equal.

KEBA © KEBA 2021

If the existing generated certificate gets invalid, then again a new certificate is generated. This will happen for example if an IP address of the device is changed, because the generated certificate lists the IP addresses of the device within the certificate. This is not the case for configured certificates. Configured certificates will never be replaced by generated certificates.

Service	Web interface
Server authentication	certificate (only for HTTPS)
Client authentication	user/password
Certificate expiration	yes
Access rights	KEBA user management

DevAdmin

The DevAdmin is a web based GUI that provides access to various information and actions of KEBA IACS components. and devices support the DevAdmin. HTTPS is the secure protocol used by DevAdmin, HTTP is only optional. The DevAdmin is based on the web interface and provides identical security properties:

Service	Web interface
Server authentication	certificate (only for HTTPS)
Client authentication	user/password
Certificate expiration	yes
Access rights	KEBA user management

Secure Shell

Secure shell (SSH) is provided by Linux based and devices. Root login and password authentication is disabled to provide a high default security level. The following SSH users exist:

- **admin**: The “admin” user has full control over the device. It is not the root user but it is allowed to open a root shell with “`sudo su -`”. The SSH key for the “admin” user can be configured during target setup with or afterwards with DevAdmin (“Administrator” role necessary).
- **service**: The “service” user has access to selected files and directories; e.g., to access log data of the machine. This user has no shell access, only file access is enabled. The SSH key for the “service” user can be configured during target setup with , afterwards with DevAdmin (“Administrator” role necessary), or by file access to authorized keys file.
- **operator**: The “operator” user has access to selected files and directories. Per default no files or directories are accessible. The accessible files and directories can be configured with . The SSH key for the “operator” user can be configured during target setup with or afterwards with DevAdmin (“Administrator” role necessary).

SSH keys do not have any expiration period. They are valid until they are replaced by new keys. Replacing the SSH keys with new ones regularly is possible and would reduce the risk of a key compromise.

© KEBA 2021

The SSH security properties are:

Service	SSH
Server authentication	host key (generated at first boot)
Client authentication	private key (public key stored on host)
Key expiration	no
Access rights	shell and file access restricted individually per user

OpenVPN

OpenVPN provides access to the machine network without having actual physical access to the machine network. The OpenVPN authentication replaces the physical access to the cabinet. Usually the OpenVPN service runs on the boundary protection device. and devices are able to act as boundary protection devices and consequently support OpenVPN.

Client and server of a OpenVPN connection authenticate each other. For authentication both check the certificate of the other for a valid certificate authority (CA) signature. Therefore, the CA certificate must be present on both to enable the signature check. The CA private key is necessary to sign the certificate of client and server.

For OpenVPN the necessary keys and certificates are generated at the first boot. First the CA private key and certificate are generated. After that, the server private key and certificate are generated and the certificate is signed with the CA private key. To enable an OpenVPN connection a CA signed client certificate is necessary. This client certificate is generated on demand. The client certificates can be managed with DevAdmin.

The highest security level for OpenVPN would be reached if the CA private key is not stored on the OpenVPN server. In this case, the server and client certificates would be signed within a protected environment with access to the CA private key. This practice would require key management external to KEBA devices and manual deployment of the keys and certificates.

If the OpenVPN keys and certificates are generated, then the CA private key is stored on the server, which is also accessed by the OpenVPN connection. Therefore, it lowers the security level compared to an external key management, but it still provides authentication and encryption of the OpenVPN connection.

OpenVPN certificates do expire. Short expiration periods provide a high security level but also a high maintenance load. Generated keys and certificates shall enable an easy use of security features. Therefore, the expiration periods of the server and the CA certificate are set to 100 years to prevent expiration in practice. The client certificates will expire after 90 days per default. This period can be increased up to 50 years. This enables the use of OpenVPN without worrying about security maintenance.

The OpenVPN security properties are:

KEBA © KEBA 2021

Service	OpenVPN
Server authentication	certificate
Client authentication	certificate
CA authentication	certificate
Certificate expiration	yes
Access rights	equal to machine network access

OPC Unified Architecture

OPC Unified Architecture (OPC UA) is a platform-independent, service-oriented architecture used for industrial automation and communication. It is the latest specification of the Open Platform Communications (OPC) standard, which is designed to facilitate secure and reliable data exchange between machines, devices, and systems from different manufacturers. It can be used to exchange data during operation and for diagnosis. OPC UA is used mostly in automation networks, but is also used in machine networks. It supports secure communication with authentication and encryption.

OPC UA requires authentication with username and password. This authentication is based on the KEBA user management. Based on roles, which are assigned to users, the access to objects and variables is granted or not. The authentication management rights mentioned above are not in use for OPC UA access control. OPC UA specific permissions are assigned individually to roles and these permission are checked on each access. This enables fine-grained access control, which ensures that only authorized users can access specific data and perform certain actions.

Additionally to username and password, there exists another layer of authentication based on certificates, which also supports encryption. OPC UA uses certificates for the authentication of both, client and server. The certificate of the communication partner needs to be known. The communication partner must prove the ownership of certificate. This prove is only possible if the communication partner knows the corresponding private key. This is valid for client and server. E.g., the server stores the certificate of the client and the client proves the ownership of the certificate. The certificates contain an application URI. This application URI is used for information purposes, like listing the connected clients. The signature of the certificates is not validated, self-signed certificates can be used.

Based on the mutual authentication with certificates a secure communication is established. This secure communication is usually encrypted and signed, which protects against eavesdropping and manipulation. Optionally, encryption can be omitted. If encryption is not used, then the communication is still signed and the integrity is still protected; i.e. data manipulation is detected.

For the OPC UA server a certificate is required. If no certificate is configured for the server, then the OPC UA server is not available. The certificate can be installed or generated with DevAdmin.

The OPC UA client is able to use multiple certificates. This is necessary, because an OPC UA client potentially connects to multiple servers and there is no guarantee that all servers are able to accept the same certificate. The

© KEBA 2021

certificates can be installed and managed with DevAdmin. The configuration of username/password combinations, which are also necessary for the authentication at OPC UA servers, is done along with all the OPC UA client configuration in .

For the substandard OPC UA PubSub authentication and encryption is specified but not implemented yet. Therefore, the use of OPC UA PubSub within the automation network is strongly discouraged. OPC UA PubSub shall only be used within the machine network by now.

For more details about the OPC UA security functions please refer to the OPC UA product documentation.

Service	OpenVPN
Server authentication	certificate
Client authentication	user/password, certificate
Certificate expiration	yes
Access rights	KEBA user management, OPC UA specific permissions based on roles

1.3.2.7 Machine network services

The machine network is an internal network of the machine or system itself. It is isolated from any other network with a boundary protection device. Usually, there exists a single boundary protection device, which connects the machine network to the automation network. If there is no boundary protection device, then there is also no machine network and services intended for the machine network shall not be used.

The machine network is a trusted zone. According to the defense in depth security strategy it shall be protected by multiple layers of firewalls and boundary protection devices. Additionally, physical access restrictions to the shop floor and even more restrictive to the cabinet are required. These measures make the following assumptions possible:

- The probability for the logical and physical presence of not authorized devices is sufficiently low to omit authentication and authorization.
- Communication within the machine network does not use untrusted channels or links. Therefore, encryption is not required for communication within the machine network.

Reliability and integrity are the objectives with the highest priority for an IACS. If the machine network would be an untrusted zone, then the required reliability cannot be reached. E.g., defined reaction times cannot be guaranteed while malicious traffic is present at the same time within the machine network. Also the physical cabling must be trusted to reach the required integrity. Therefore, it is necessary to implement the machine or system and subsequently also the machine network as a trusted zone. Thus, the machine network provides a higher security level by design and the security requirements for services within the machine network are lower compared to the automation network.

KEBA © KEBA 2021

KEBA and devices can be used as boundary protection devices for machine networks. In this case, the firewall must be configured to provide only secure services to the automation network. Other none secure services are then only provided to the machine network.

If there is a machine network with a boundary protection device, then the use of the services listed below within this network is allowed. The automation network services listed above can also be used in the machine network, because the security requirements for the machine network are lower than for the automation network.

Each machine network services provided by KEBA IACS components has specific security properties. These specific security properties need to be known to decide if a service should be used and how it is configured to provide the required security level. The product documentation will indicate whether a particular service is supported or not.

Field buses

Field buses are used only within machine networks. Various types of field buses exist, but they do have common properties. Field bus devices are only identified and not authenticated. Communication is not encrypted and has to fulfill real-time properties. As the machine network is a trusted zone, the use of field buses is allowed even with the lack of advanced security measures.

The communication on field buses is usually reduced to a minimum, which is beneficial for security. The content of the communication needs to be configured and cannot be extended arbitrarily during runtime. Thus, this configuration is in line with the principle of least privileges.

Some field buses support Ethernet based communication; e.g., EtherCAT supports EoE (Ethernet over EtherCAT). This Ethernet based communication has to be limited to the machine network. KEBA boundary protection devices like and products do limit this Ethernet based communication to the machine network.

The security properties for field buses are:

Service	Display and operating elements
Application authentication	geographical location, machine network
Access rights	no restrictions

RPC

KEBA and provide RPC based services. These RPC based services provide a broad range of features supported by these devices. All these services are KEBA specific, only RPC itself is a standardized protocol (Remote Procedure Call)

The RPC protocol does not support any security features like authentication and encryption. Thus, the use of RPC and the services based on it shall be limited to a trusted zone like the machine network. The use of RPC and the services based on it within the automation network or any other network without any additional security measures is strongly discouraged.

© KEBA 2021

KEBA tools like use RPC to communicate with KEBA devices. If the RPC protocol is restricted to the machine network by a firewall for example, then the tools communication is only possible if the tools software has access to the machine network; e.g., the laptop with the installation is connected to the “Ethernet 1” port of the device. OpenVPN can be used to gain access to the machine network without physical access. In this case, OpenVPN is the additional security measure which allows the use of RPC within other networks than the machine network.

The RPC security properties are:

Service	Display and operating elements
Application authentication	geographical location, machine network
User authentication	geographical location, machine network
Access rights	no restrictions

KVC

The KVC protocol is a KEBA specific protocol for the communication between devices and devices. KVC is the abbreviation for KEBA Virtual Channel. This virtual channel is used to:

- get the status of keys
- set the status of LEDs
- get the orientation of the device
- get the status of the handwheel
- …

The KVC protocol does not support any security features like authentication and encryption. Thus, the use of KVC shall be limited to a trusted zone like the machine network. The use of this service within the automation network or any other network is strongly discouraged.

The KVC security properties are:

The KVC security properties are:

CODESYS

KEBA and a limited set of devices support the CODESYS runtime system. For the communication with the CODESYS runtime system a specific set of communication protocols is in use. This set is calles CODESYS communication protocols.

The CODESYS communication protocols does support authentication. Encryption is not in use. Thus, the use of CODESYS communication protocols shall be limited to a trusted zone like the machine network. The use of CODESYS communication protocols within the automation network or any other network without any additional security measures is strongly discouraged.

KEBA © KEBA 2021

KEBA tools like use the CODESYS communication protocols to communicate with KEBA devices with CODESYS runtime. If the CODESYS communication protocols are restricted to the machine network by a firewall for example, then the tools communication is only possible if the tools software has access to the machine network; e.g., the laptop with the installation is connected to the “Ethernet 1” port of the device. OpenVPN can be used to gain access to the machine network without physical access. In this case, OpenVPN is the additional security measure which allows the use of CODESYS communication protocols within other networks than the machine network.

The CODESYS communication protocols security properties are:

Service	Display and operating elements
User authentication	user/password
Access rights	no restrictions

EtherCAT mailbox gateway

The EtherCAT mailbox gateway service provides access to the mailbox of EtherCAT slaves. This direct access is usually used to configure EtherCAT slaves with functional safety features. In this case the AoE mailbox protocol is used.

The EtherCAT mailbox gateway protocol does not support any security features like authentication and encryption. Thus, the use of the EtherCAT mailbox gateway shall be limited to a trusted zone like the machine network. The use of this service within the automation network or any other network without any additional security measures is strongly discouraged.

KEBA tools like SafeEdit NG use the EtherCAT mailbox gateway to communicate with KEBA functional safety devices. If the EtherCAT mailbox gateway is restricted to the machine network by a firewall for example, then this tools communication is only possible if SafeEdit NG has access to the machine network; e.g., the laptop with the SafeEdit NG installation is connected to the “Ethernet 1” port of the device. OpenVPN or other secure tunnels like SSH can be used to gain access to the machine network without physical access. In this case, the secure tunnel is the additional security measure which allows the use of RPC within other networks than the machine network.

The EtherCAT mailbox gateway security properties are:

Service	Display and operating elements
Application authentication	geographical location, machine network
User authentication	geographical location, machine network
Access rights	no restrictions

PLC protocols for non-KEBA PLCs

For the communication of devices with non-KEBA PLCs multiple protocols are supported:

- ADS (Beckhoff PLC)

© KEBA 2021

- S7 (Siemens PLC)
- Modbus

Similar to KVC, these protocols are used to:

- get the status of keys
- set the status of LEDs
- get the orientation of the device
- get the status of the handwheel
- …

These PLC protocols for non-KEBA PLCs do not support security features like authentication and encryption. Thus, the use of these protocols shall be limited to a trusted zone like the machine network. The use of PLC protocols for non-KEBA PLCs within the automation network or any other network is strongly discouraged.

The security properties of PLC protocols for non-KEBA PLCs are:

Service	Display and operating elements
Application authentication	geographical location, machine network
User authentication	geographical location, machine network
Access rights	no restrictions

1.3.2.8 Wireless interfaces

Besides wired interfaces like Ethernet and CAN, also wireless interfaces are supported for selected KEBA IACS components. Special attention is necessary for the security of wireless interfaces, because physical access restriction is not always possible for this type of interfaces.

RFID

SelectedKEBA IACS components have an RFID interface to read information from RFID cards. This information is typically used for user authentication and needs to be protected.

The range of RFID is less than one meter. Due to this limited range, physical access restriction is a valid security measure for RFID. Thus, the owner of an RFID card is able to protect the information of their RFID card by restricting the access to their RFID card.

Most of the time information is only read from the RFID card. Sometimes information is written to the RFID card. In both cases only a limited amount of data is transferred. No communication protocol established, which would provide access to network services. Due to these facts, no additional security measures like authentication and encryption are necessary for RFID.

WLAN

The range of WLAN is more than 10 meters. Therefore, physical access restriction for WLAN is not possible. For KEBA IACS components, WLAN interfaces are considered as interfaces to the automation network. Thus, the se-

KEBA © KEBA 2021

curity level required for communication protocols on the WLAN is identical to the requirements for communication protocols on the automation network. Authentication and encryption is recommended for communication on the WLAN.

No matter which communication protocols are used, the WLAN itself should be authenticated and encrypted. It is the responsibility of the operator of the access point, which is often the asset owner, to configure the required level of security.

WLAN access point for KeControl

devices are able to operate as access points if the installed software supports this feature. To enable the access point, it is sufficient to plug a supported USB WLAN adapter to a USB port. The access point starts automatically with a WPA protected WLAN. The SSID is the MAC address of the used USB WLAN adapter and the passphrase is the serial number of the device.

Similar to normal WLAN interfaces, also the WLAN of this access point is considered as automation network. Thus, the security level required for communication protocols on the WLAN is identical to the requirements for communication protocols on the automation network. Authentication and encryption is recommended for communication on the WLAN.

With the firewall, the protocols in the WLAN can be restricted to secure protocols. This way, the security of communication is independent of the WLAN security. This is an important property as the WPA passphrase is not random. Therefore, it is recommended that the firewall restricts the communication on the WLAN to secure protocols if the WLAN access point feature is in use.

Wireless KeTop system

If the wireless system consisting of an handheld terminal and a basestation is used as a cable replacement, the connection is authenticated (kept together) and encrypted by the pairing process. In another use case, all the network precautions described must be observed.

1.3.2.9 Physical interfaces

KEBA IACS components have physical interfaces in addition to the already discussed network services. The specific security properties of these physical interfaces need to be known to decide if a physical interface should be used and how it is configured to provide the required security level.

Display and operating elements

User interfaces like display with keys, wheels, … are authenticated first by geographical location. Access to the shop floor is needed to access the GUI and buttons of a KEBA device. Furthermore, access to the cabinet is needed to access display and buttons of and devices.

© KEBA 2021

Visualization devices accessible on the shop floor like s often require an additional authentication to enable more or the full range of functions. Passwords and key cards are commonly used for this additional authentication. Based on this authentication, the roles and the users are checked for visualization specific user level rights of the visualization. Based on the assigned user level rights, the visualization application allows access to certain features or not.

Visualization applications are always full-screen. They do not allow access to the operating system desktop to start and stop arbitrary applications. If multiple visualization applications are supported, then a kiosk desktop is used. A kiosk desktop only allows to execution of selected applications – these are installed and configured on the device by the administrator or application developer, not by the standard user.

If the visualization is a web interface based application, then user level rights are not sufficient. The web interface checks for other rights than user levels and denies access if the needed rights are missing. Thus, the visualization application also has to authenticate the user against the web interface to enable the use of features which require the web interface.

The security properties for displays and operating elements are:

Service	Display and operating elements
Application authentication	geographical location
User authentication	geographical location, optionally password or key card
Access rights	defined by application, KEBA user management for web based application

USB interfaces

USB interfaces are authenticated at least by geographical location. A user must be able to plug a cable or a device into the USB connector. USB interfaces provide a broad range of functions. These functions can be grouped in the following way:

- **USB host interface**: The USB port is used to connect USB devices like USB thumb drives and access them from applications running on top of an operating system. The actual functions accessible vary a lot; e.g. a USB thumb drive can be used to provide files or to automatically install software.
- **USB device**: The USB port provides access to a well-defined USB device. This is the opposite to the USB host interface. The USB device is connected to an USB host interface. The USB network interface is an example for an USB device. It provides a USB based network interface to a service laptop.
- **USB boot**: The operation system on the USB thumb drive is booted directly by the BIOS or bootloader. This a special function of a USB host interface.
- **USB BIOS keyboard**: BIOS menu is accessed with keyboard connected over USB.

KEBA © KEBA 2021

This list shows that USB is used for various functions. The easy-to-use nature of USB facilitates its broad use.

Some functions available on USB provide powerful access to the device. Therefore, it is recommended to keep the USB ports within the cabinet, which enforces a high level of physical access protection. Only if the required security level is sufficiently low and the physical access protection to the shop floor is high enough, then USB ports can be made accessible directly on the shop floor.

1.3.2.10 Visualization frameworks

KEBA provides visualization frameworks like e.g. KeView Style and KeView Trend to build visualizations and ready to use visualization like e.g. TeachEdit. The boundary between frameworks and visualizations is blurring. Visualization frameworks can provide ready to use masks and dialogs. Ready to use visualizations can be controlled with parameters and extended with customer code. For both, frameworks and visualizations, the following security rules shall be considered:

- **Secure tunnel**: If the visualization application runs outside of the machine network and uses services without authentication and encryption to communicate with the PLC, then the communication needs to be secured with a secure tunnel. This is the case for all visualization applications not based on web interfaces. OpenVPN can be used as a secure tunnel. If the visualization application runs directly on the PLC or on a handheld terminal within the machine network, then a secure tunnel for the communication is not needed.
- **Web resources**: If the visualization is browser based, then HTTPS shall be used and all resources used by the web application shall be hosted within the machine network. There shall be no scripts, images, stylesheets, fonts, REST APIs, WebSocket APIs, … hosted within the automation network, the IT network or even worse the internet. This is necessary to eliminate the threat of malicious input to the browser, which is the most common security vulnerability for browsers. This also includes browsing the internet or any other untrusted website. KEBA visualization software, which includes a browser, runs in kiosk mode to prevent the escape of the user to arbitrary websites. Browsing untrusted websites like the internet is out of scope for any browser based visualization software.

1.3.2.11 Tools

The KEBA tools are able to communicate with the KEBA devices over secure protocols. Two variants of secure communication exists. The first variant is the use of protocols, which are secure by design. The second variant is to use OpenVPN to tunnel insecure protocols between tools PC and KEBA device.

To ensure that only secure protocols are used on the automation network for tools communication, the firewall of the KEBA devices shall be configured to allow only secure protocols. This way protocols with weak or no security cannot be used by accident.

© KEBA 2021

1.3.2.12 Software updates

Software needs to be updated to new versions from time to time. There are multiple reasons for a software update:

- **Fixed security bug**: A security bug, which is relevant to the actual application of the software, is fixed in the new version.
- **Fixed functional bug**: A functional bug, which has negative impact to the operation of the software, is fixed in the new version.
- **Additional feature**: The new version includes a new feature, which is required by users or is required to enable other enhancements depending on this feature.
- **Increased support period**: The end of the support period of the current version is near and the software shall still be used in the future.

Updates can be done on demand or on a regular base. To keep the software in use secure, regular update are recommended.

KEBA uses state of the art development processes to minimize the risk of security and functional bugs. Despite that, bugs cannot be prevented completely. These remaining bugs potentially can be exploited to break the security of a device; e.g., to execute actions without the necessary authentication. Software updates are the widespread and recognized way to fix bugs in the field. Therefore, software updates are possible for every KEBA IACS component.

1.3.3 Defense in Depth

Defense in depth is a security strategy, which uses multiple layers of security to tolerate single security issues or bugs. Single security holes like software vulnerabilities will appear. As a result, only additional security layers can reduce the security exposure when a security hole is present. Also, IEC 62443 defines defense in depth as its security strategy. Therefore, it is assumed that defense in depth is implemented by the asset owner, the system integrator and the machine builder. KEBA products support various security layers, which facilitate the implementation of the defense in depth strategy.

There are various options to implement security layers. These options can be grouped into physical and logical security layers. Physical security layers are implemented at different locations, mostly within the environment and at IACS level. Examples are gates at premises and buildings that can only be passed with valid key cards. Also door locks for cabinets are physical security measures. Logical security measures are more diverse and can be grouped by location:

- **Environment:** In the environment, logical security layers in the form of firewalls are implemented. They establish zones, which can prevent the propagation of security threats.
- **IACS:** At industrial automation and control system level, security layers in the form of authentication, encryption and least privilege are used. Firewalls are also relevant for IACS.

KEBA © KEBA 2021

- **IACS component:** Similar to an IACS, its components implement security in the form of identification, authentication, encryption, least privilege and auditing. Additionally, integrity checks are used as security layer.

1.3.4 Protected environment

The environment for the operation of an IACS has big influence on the reachable security level. If for example everyone has physical access to the cabinet of a machining center, then a high security level cannot be achieved. With physical access to the cabinet by everyone, the cabling could be manipulated easily with serious consequences. Therefore, allowing physical access only to a restricted group of people is a common measure to provide a minimum level of security. Which measures are taken depends on the security level that shall be reached. This target security level is defined by the asset owner of the IACS.

A single IACS component cannot guarantee a certain security level for the whole IACS. The threats and the necessary measures to counter them depend heavily on the application and often need to be implemented on system level. In the end, an IACS is always operated within a protected environment, because the threats and risks cannot be mitigated in an arbitrary environment. Thus, a protected environment is a reasonable assumption and can be set as precondition for the secure operation of IACS components.

The security measures established within this protected operating environment are derived from the required security level of the asset owner. Every asset owner has to find the right balance between enough security measures, which establish the required security level, and not too many security measures, which will increase the cost (operation, service, …).

The following list provides an overview over common security measures:

- **Physical access control to shop floor:** Only people who are allowed to access the shop floor are able to access the shop floor.
- **Physical access control to cabinet of machine:** Only people who need to do work within the cabinet are able to open the cabinet.
- **Password policies:** Passwords shall be strong and kept as personal secret.
- **Isolated network for the shop floor:** The network, which connects the machines on the shop floor (automation network), shall be isolated from all other networks like the IT network by a firewall. An IACS shall never be operated in open networks or in the internet. This also enhances the reliability of the network.
- **Secure communication:** Use authenticated and encrypted communication mechanisms like OPC UA, HTTPS, VPN, or SSH to communicate with the IACS.
- **Expose minimal set of interfaces:** Don’t expose interfaces of IACS components like USB or network ports on the shop floor. The only exception are USB ports of and devices, which are designed for this use case.

© KEBA 2021

- **IT security measures for IT devices:** Use state of the art IT security measures for IT devices no matter if they are located within the IT network or the network on the shop floor (automation network). Especially IT devices, which are able to connect to IACS components, need to be considered as their security level has direct influence on the security level of the IACS components. An example for an IT security measure is to run virus scanners on desktop PCs used on the shop floor. Be aware that for IACS components, IT security measures like virus scanners are often not suitable. Especially PLCs cannot be treated like IT devices.
- **Recovery:** In case of a security incident, the goal is to bring all systems back to normal. Therefore, a recovery strategy is needed. Backups are often an important part of the recovery strategy. Tests are required to ensure that the recovery procedures actually work when they are needed.

The actual selection of the security measures and the calculation of the overall reached security level is done by the asset owner.

1.3.5 Network architecture

It is very common for machines to communicate on the shop floor. They communicate for example with SCADA systems during production and also with tools for diagnosis. This network on the shop floor is the automation network. As mentioned above, this automation network shall be isolated from other networks for security and reliability reasons. The communication interface of the machine to the automation network forms a boundary between the machine and the automation network. All communication over this interface is highly security relevant. Therefore, all protocols used on this interface shall be known and selected with security in mind.

The communication interface of the machine to the automation network is often more than just a boundary between the machine and the shop floor. Machines often include an internal network between its IACS components. In this case the communication interface is a boundary between two networks, the internal machine network and the external automation network. But no matter whether the machine consists of single PLC or multiple IACS components, the communication over this interface is highly security relevant in both cases.

A machine without an internal machine network is a special case, which does not need to be considered separately. It is just the absolute minimum of an internal machine network. It does not expose additional security risks compared to a machine with an internal machine network. As soon as any field bus communication is used, an internal machine network is established. Thus, a machine without an internal machine network is a very rare case. Overall, it is safe to assume that this special case does not need any further attention and is included within the consideration about machines with internal network.

KEBA © KEBA 2021

Network naming

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:

- **Automation network**
- Production site network
- Control network
- Shop floor network
- Production network
- Factory network
- External network (external to the machine)
- Internal network (internal to the factory)

Again without any claim to completeness, for the internal network of the machine the following names might be used:

- **Machine network**
- Internal network

This document uses the names "automation network" and "machine network".

Boundary protection device

The connection between automation network and machine network is done by a device, which is connected to both networks. This device will be called boundary protection device in this document. The boundary protection device role can be filled by any device, which is able to operate within both networks. Be aware that the machine network can be a field bus, an IP based network or a combination of networks of both types.

Here a list of boundary protection device examples for better understanding. The examples can be combined for more complex systems:

- PLC: Ethernet interface for automation network and EtherCAT interface for machine network with IOs and drives.
- Active operating panel: Ethernet interface for automation network and Ethernet interface for machine network with PLC.
- Gateway: Generic gateway device with Ethernet interface for automation network and Ethernet interface for machine network with PLC.

For the automation network usually a higher security level is required than for the machine network, because its exposure to security threats is higher. As the boundary protection device is part of both networks, the security requirements for the boundary protection device are higher than for other de-

© KEBA 2021

vices within the machine network. The boundary protection device has to reach the security level required for the automation network. Therefore, the security of the boundary protection device is taken into account separately.

Network segmentation

The boundary protection device enforces a segmentation between automation network and machine network. Network segmentation provides advantages for security, reliability, and service. For security it reduces the exposure and the spread of the machine network to the automation network. Services can be provided only for the machine network. IACS components within the machine network cannot access the automation network in arbitrary ways, because the boundary protection device limits that access.

Reliability is improved, because the traffic within the networks is reduced. Local traffic within the automation network is kept within the automation network and does not affect the machine network. This is also valid for the machine network vice versa.

Also service and maintenance is simpler if the machine appears as a single device within the automation network. An automation network specific IP address only needs to be assigned to the boundary protection device of the machine. The IACS components within the IP based machine network use private IP addresses, which cannot conflict with IP addresses on the automation network. Otherwise all IACS components within IP based machine network would need automation network specific IP addresses. This would lead to increased effort and complexity when the machine is brought into service.

As soon as the boundary protection device acts as router/gateway, these advantages of the network segmentation are considerably reduced. Most relevant in this case is that direct communication between the segments is now possible, which otherwise is not. If the boundary protection device acts as switch, then there is no network segmentation and none of the advantages are valid.

The network segmentation enables the realization of zones and conduits as recommended for the threat and risk assessment of the IACS.

Network topology

Network topology is the arrangement of the elements of the communication network. The arrangement and elements used vary in numerous details for every network. From an overview perspective the differences become smaller and common properties get visible. Therefore, it is possible to define a reference network topology, which fits to the majority of existing communication networks.

The reference network topology assumed for an IACS with KEBA products is shown in the following figure.

KEBA © KEBA 2021

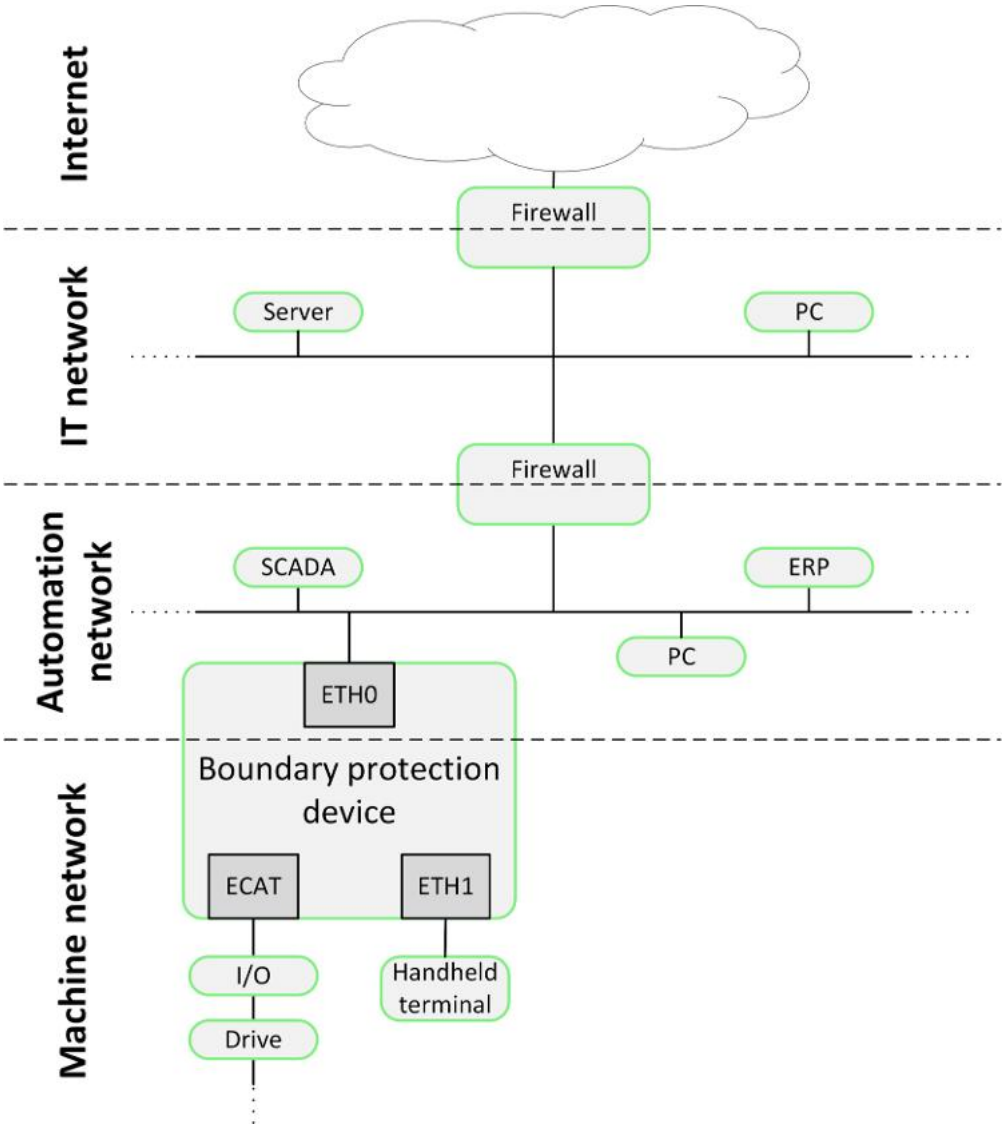


Fig. 1-1: Reference network topology

The Internet is the global network, which connects offices, factories, devices, … around the world. The Internet is not trusted. While the internet offers many benefits, its security is still evolving, with ongoing challenges like data breaches, misinformation, and the need for stronger encryption and authentication measures. Therefore, the Internet is a network that can not be trusted.

The IT network is connected to the Internet. It is a separate network segment, which is protected by a firewall to reach the required security level of the asset owner. The figure above shows a simple IT network. Often, IT networks consists of multiple network segments like a separate zone for servers.

The IACS is not located within the IT network. The IACS is realized within the automation network, which is again a separate network segment isolated from the IT network with a firewall. Within the automation network one or more IACS exist. These IACS consist of machines, devices or other equipment. A single machine can also be an IACS.

© KEBA 2021

As already mentioned, the internal network of a machine is called machine network. This network is connected to the automation network with a boundary protection device, to separate these network from each other. Multiple machine networks can be connected to a single automation network.

Network services

Machines can provide services to the automation network. Those services can be used during operation or on demand e.g. for diagnosis. The services are provided by the boundary protection device, because the network segmentation enforces that only the boundary protection device has access to the automation network. Other IACS components within the machine network cannot provide services directly to the automation network. Every service increases the security exposure of a device and also for the boundary protection device, of course. Therefore, the provided services shall be reduced to the necessary minimum.

If a service of an IACS component within the machine network shall be provided on the automation network, then the boundary protection device has to forward this service. This forwarding can be done in a generic way on IP level (layer 3) or in a protocol-specific way. The generic forwarding on IP level leads to a high exposure of the IACS component to the automation network. Protocol-specific forwarding like e.g. HTTP forwarding leads to a lower exposure compared to generic forwarding, but cannot be applied to any protocol.

The boundary protection device can provide services to the automation network and to the machine network, because it is connected to both networks. Common default is that services are provided to all connected networks. Due to the network segmentation done by the boundary protection device, the security considerations for both networks usually differ. Thus, a service which is secure enough for one network is not necessarily secure enough for the other network. The exposure of the automation network is higher than the exposure of the machine network. Thus, a service can be secure enough for the machine network, but not for the automation network. Therefore, it can be a security problem if every service of the boundary protection device is provided to the automation network. The solution is to provide only a subset of all activated services of the boundary protection device to the automation network. This is usually done by a firewall on the boundary protection device. Also, binding services only to the interface of the machine network is a valid solution.

Outbound network communication

In addition to network services, there is outbound network communication, which is also relevant for security. Every network communication is threatened by eavesdropping, spoofing, tampering, …. Therefore, it is a general security principle to reduce the network communication to the necessary minimum. As mentioned above, the exposure of the automation network is higher than the exposure of the machine network. Thus, it makes sense to pay special attention to the used communication on the automation network. Due to the network segmentation, only the boundary protection device is able to communicate to the automation network. Therefore, limiting the com-

KEBA © KEBA 2021

munication initiated by the boundary protection device to the automation network limits the whole communication initiated by the machine to the automation network.

Network services usually can be enabled and disabled by configuration of the IACS component. Similar outbound network communication usually needs to be enabled by configuration; e.g., the configuration of an NTP server IP address enables the communication with this server. Additionally, outbound network communication can be triggered by applications. This can happen either directly or indirectly. A network communication is triggered directly by programming against a socket API; e.g. the Linux POSIX socket API. Indirect triggering happens by using an API function which internally uses the socket API; e.g. by using an FTP library.

1.3.6 Network properties

The networks of the production site like the automation network and the machine networks enable cost efficient production and are critical for the economic success. Availability and integrity usually have a higher priority than confidentiality. In contrast, for IT networks confidentiality is typically the most important objective. Therefore, production site networks have different properties when compared to IT networks.

Production site networks are nearly always protected by physical access control. Only authorized persons can access the network hardware and network ports. This protection is usually more strict than for IT networks, which are present in offices and also in meeting rooms used for guests.

Automation network

The automation network is the network on the shop floor, which enables the communication of machines, SCADA, workstations and other devices required for operation. Secure protocols like OPC UA are available for the communication on the automation network. The usage of secure protocols requires the management and maintenance of keys. Individual keys which are changed regularly provide a high security level. The key management requires continuous efforts. If the key management fails, then the security level is decreased and in worst case the production is stopped due to failed authentication. Thus, software support to simplify key management is required.

Besides secure protocols, other security measures can be used to reach a satisfying security level for the asset owner. Passwords are still a valid security measure. The risk of password eavesdropping can be reduced by restricting the communication flow within the automation network. Also, IP range restrictions reduce the attack surface of protocols.

The automation network is a separate network which is isolated from the IT network by a firewall. This is necessary as the availability and responsiveness requirements of the automation network are higher than for the IT network. Furthermore, security is also improved by this firewall, because communication is restricted to certain protocols and eventually also to selected IP ranges.

© KEBA 2021

Machine network

The machine network is an internal network of the machine and very specific to the actual machine type. Established IT security measures like encryption and authentication often cannot be used all over the machine network. The properties of the machine network are similar to the automation network, but the requirements for availability and responsiveness are higher.

Within the machine network, field buses like e.g. EtherCAT are in use. These field buses are designed for robust real-time communication. Confidentiality of the communication was no design goal. The data communicated over field buses is valid at a certain instant of time; e.g., the position of the robot. Additionally, the interpretation of this data requires deep knowledge of the machine and only historical data can be reconstructed. Thus, this data does not require confidentiality. Additionally, the CPU performance required for encryption of real-time communication would increase the costs of the IACS components significantly.

Encryption and authentication of communication requires key management. Every IACS would need one or more keys. As mentioned above, this key management requires continuous effort. But the more important fact is, that IACS components cannot be replaced easily anymore. The replacement would also require the deployment of the keys to the new IACS component. This complicates service and maintenance and is often not feasible.

Within the machine network and particularly for field buses the communication has to satisfy real-time requirements. Even disturbing this communication only slightly can cause real-time violations and would lead to a machine stop. Thus, real-time communication shall be isolated in any case to guarantee the correct timely behavior.

To sum up, within the machine network, the communication cannot be based solely on protocols with authentication and encryption. The boundary protection device isolates the machine network from the automation network and enables dedicated security measures for the machine network. The physical access control for the machine network is usually more restricted than for the automation network. Also it is best practice, that direct communication with IACS components within the machine network is not possible for devices not connected to the machine network. The boundary protection device does not act as router and limits communication to the machine network.

1.3.7 Remote access

For some use cases it is necessary to connect to the machine network without physical access to the machine network; e.g., for remote configuration or diagnosis with software tools. These connections are established on demand and are time limited. Various solutions exist to securely connect over untrusted networks. All solutions have in common that a terminal service must run on an IACS component within the machine network. Usually it runs on the boundary protection device. A software tool of the selected solution is required on the connecting device.

KEBA © KEBA 2021

If the boundary protection device is directly accessible by IP address, then widely used virtual private network (VPN) protocols can be used. The VPN provides an authenticated and encrypted connection to the machine network. Services, which are available within the machine network, can be made available also over the VPN connection. With VPN it is possible to access services of IACS components including the boundary protection device, which can provide more services to the machine network than to the automation network.

Often the boundary protection device is not directly accessible by IP address. This is the case if the machine is located at a production site of a different company. An automation network is nearly always a private network, which cannot be reached over the internet. Therefore, direct access is only possible within the network of the machine owner. As a consequence, an agent, which arranges the connection, is necessary. This agent is an internet service, because the internet is the only common network available for the terminal service within the machine network and the software tool on the connecting device. Both, the terminal service and the software tool connect to the agent. These connections must be authenticated and encrypted as the internet is an untrusted network. The agent establishes a connection by forwarding the communication between them in both directions. This mechanism enables connections which are not possible with VPN. The operation of the agent generates costs for traffic, storage, and maintenance.

Both solutions, VPN and the connection over an agent, provide complete access to the machine network. This is intended as this complete access is necessary for diagnosis and maintenance tasks. But this also bears some inherent security risks as the services within the machine networks usually implement less security measures than services in other networks. Thus, special care is needed to ensure that these remote connection do not increase the attack surface. E.g., the laptop used for the remote connection must be secured with IT security measures.

1.3.8 Reference IACS

For the discussion of security properties of an IACS and its components a common understanding of the topology of an IACS is required. A reference IACS, which subsumes the actual IACS topologies, is helpful.

The following figure shows a reference IACS.

© KEBA 2021

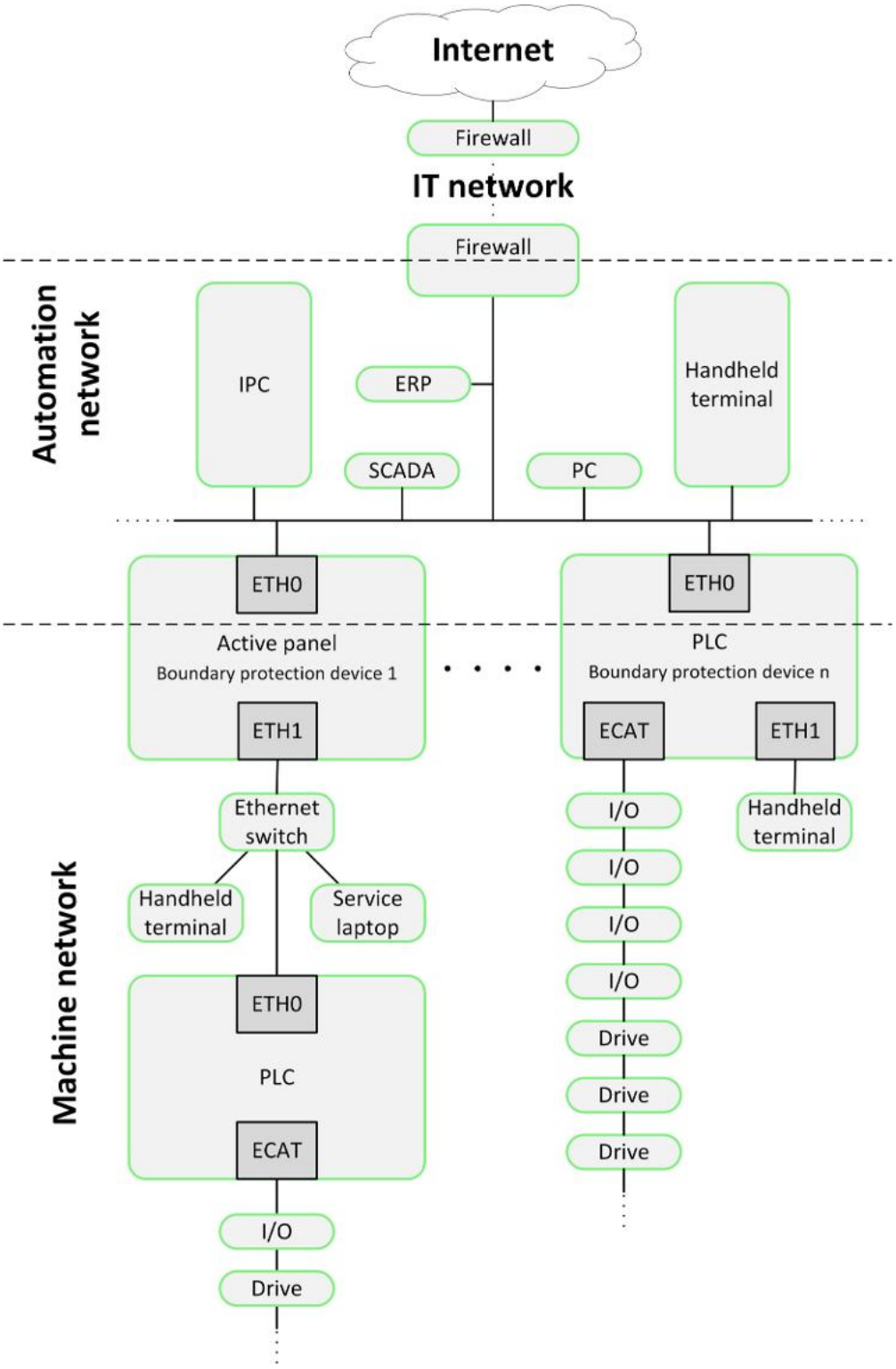


Fig. 1-2: Reference IACS

The figure above shows such a reference IACS. The backbone of the IACS is the automation network. The automation network is connected to the IT network and to the Internet and all networks are isolated from each other by firewalls. Within the automation network the high level functionality of the

KEBA © KEBA 2021

IACS is established by machines and other equipment communicating with each other. There can be equipment like IPCs and handheld terminals within the automation network. Machines and equipment with an internal machine network are connected to the automation network by a boundary protection devices. There can be one or more boundary protection devices. Every boundary protection device connects a separate machine network. The machine networks are not connected to each other.

Machine networks vary a lot. They may contain field bus networks like EtherCAT segments with IO and drives. Also Ethernet networks for service laptops, handheld terminal and other Ethernet based devices are possible. PLCs and active panels, which can act as boundary protection devices, can be used within the machine network too without being connected directly to the automation network. The actual machine network in individual to machines and equipment. Therefore, it can only be outlined using examples.

1.4 Notes on this document

This manual is an integral part of the product. It is to be retained over the entire life cycle of the product and should be forwarded to any subsequent owners or users of the product. For end users, necessary safety notes and information must be integrated in the instruction manual for end users in the specific national language by the mechanical engineer or the system provider.

This documentation must be legible and available to the specified persons and must be read and understood by them.

Information

This manual also applies to the customer variants that are identical in construction and function.

Because these types of customer variants occasionally differ from the KEBA standard variant in their appearance (e.g. due to a different front membrane), the devices pictured in this manual may differ in appearance from the devices you are using.

Information

In case of deviations of customer variants from the KEBA standard variant, a customer data sheet can be obtained from KEBA.

1.4.1 Contents of document

- Safety notes and transport conditions
- General product description
- Display, operating elements and keypad
- Connection and wiring

© KEBA 2021

- Configuration and operating instructions
- Options
- Accessories
- Technical data
- Declaration of conformity, directives and standards

1.4.2 Not contained in this document

- Mask description of the application
- Application-specific industry software

1.5 Documentation for further reading

Doc. No.	Designation	Target group
1008551	KVC protocol	Start-up technician, programmer
1008882	Modbus protocol	Start-up technician, programmer
	ADS protocol	Start-up technician, programmer
	OPC UA protocol	Start-up technician, programmer
	S7 protocol	Start-up technician, programmer
	Quick Start Guide	Start-up technician, programmer

Certificates (e.g. UL certificate) that may be required can be obtained from KEBA upon request and/or are listed in the UL product database.

1.6 Conformity of safety fieldbusses

1.6.1 EtherCAT declaration

EtherCAT®	EtherCAT® is registered trademark and patented technology, licensed by Beckhoff Automation GmbH, Germany.
Safety over EtherCAT®	Safety over EtherCAT® is a registered trademark and patented technology, licensed by the Beckhoff Automation GmbH, Germany.

KEBA © KEBA 2021

1.6.2 PROFINet / PROFIsafe declaration

	PROFINet® is a registered trademark. Use is only permitted for members of "PROFIBUS & PROFINET International". More information about the terms of use can be found on the web page www.profibus.com.
	PROFIsafe® is a registered trademark. Use is only permitted for members of "PROFIBUS & PROFINET International". More information about the terms of use can be found on the web page www.profibus.com.

1.7 Information in relation to MRL 2006/42/EC

This user's manual corresponds to machinery directive 2006/42/EC.

1.7.1 Quantitative safety relevant specifications for emergency stop-button and enabling device

Emergency stop and enabling switch

KEBA specifies a category and a PL in acc. with EN ISO 13849-1 and a PFH_D value and an SIL rating in acc. with EN 61508.

Information

Enabling switch circuits and emergency stop circuits consist of a combination of mechanical elements and electronic evaluations.

1.7.2 Relationship between Performance Level and Safety Integrity Level

Table 3 (acc. to EN ISO 13849-1:2015) - Correlation of Performance Level (PL) and Safety Integrity Level (SIL)

Performance Level (PL) by EN ISO 13849-1	Safety Integrity Level (SIL) by EN 61508-1
a	no corresponding value
b	1
c	1
d	2
e	3

© KEBA 2021

Table 2 (acc. to EN ISO 13849-1:2015) - Performance Level (PL)

Performance Level (PL)	Average probability of a dangerous breakdown per hour 1/h
a	≥ 10^{-5} to < 10^{-4}
b	≥ 3 x 10^{-6} to < 10^{-5}
c	≥ 10^{-6} to < 3 x 10^{-6}
d	≥ 10^{-7} to < 10^{-6}
e	≥ 10^{-8} to < 10^{-7}

1.7.3 Abbreviations

Abbreviation	Term	Meaning
B_{10D}	-	Number of cycles until 10% of the components fail dangerously (per channel)
$MTTF_D$	Mean time to Failure Dangerous	Mean time to dangerous failure (per channel)
DC	Diagnostic Coverage	Diagnostic coverage
PL	Performance Level	Discrete level that specifies the capacity of safety devices to execute a safety function under foreseeable conditions.
PFH_D	Probability of Failure per Hour Dangerous	Average probability of a dangerous failure per hour
SIL	Safety Integrity Level	Safety integrity level
t_{Cycle}	-	Average time between two consecutive cycles in seconds
h_{op}	-	Average operating time in hours per day (0 - 24 hours)
d_{op}	-	Average operating time in days per year (0 - 365 days)
n_{op}	-	Average number of switching cycles per year

1.8 Emergency stop switch

The emergency stop on the handheld device and on the base station corresponds to the requirements of EN ISO 13850. Based on the risk assessment for the machine, the operating principle of the emergency stop must be designed as a stop of Category 0 or Category 1 (see EN 60204-1). The relay contact wiring must fulfill the specific category (in acc. with EN ISO 13849-1) that is defined based on the risk analysis of the machine (in acc. with EN ISO 12100:2010).

KEBA © KEBA 2021

WARNING!

- Non-functional emergency stop systems can have fatal consequences! Emergency stop switches marked in red-yellow must be effective at all times and in all operating modes of a machine or system.
- An unlocking of the emergency stop system must not trigger an uncontrolled restart.
- The emergency stop is no substitution for safety systems.
- Certain mechanical errors in the emergency stop can only be detected during operation.
  After heavy impact on the device (e.g. due to an impact effect), the emergency stop switch must be checked for functional integrity. Additionally, the emergency stop must be periodically tested (every 1 month) by actuating the emergency stop switch.
- For further information on the emergency stop, be sure to observe Chap. "EU Directives, Standards and Regulations."

© KEBA 2021

2 Safety notes

2.1 Representation

At various points in this manual, you will see notes and precautionary warnings regarding possible hazards. The symbols used have the following meaning:

DANGER!

indicates an imminently hazardous situation, which will result in death or serious bodily injury if the corresponding precautions are not taken.

WARNING!

indicates a potentially hazardous situation, which can result in death or serious bodily injury if the corresponding precautions are not taken.

CAUTION!

means that if the corresponding safety measures are not taken, a potentially hazardous situation can occur that may result in slight bodily injury.

Caution

means that damage to property can occur if the corresponding safety measures are not taken.

ESD

This symbol reminds you of the possible consequences of touching electrostatically sensitive components.

Safety information

Describes important safety-related requirements or informs about essential safety-related correlations.

Information

Identifies practical tips and useful information. No information that warns about potentially dangerous or harmful functions is contained.

KEBA © KEBA 2021

2.2 General safety instructions

The handheld terminal has been developed, manufactured, tested and documented in accordance with the ergonomic principles for design and appropriate safety standards. Therefore, provided that the instructions and safety precautions relating to the intended use are observed, the products do not pose any danger to the health of personnel or a risk of damage to other property or equipment under normal circumstances.

The instructions contained in this manual must be precisely followed in all circumstances. Failure to do so could result in the creation of potential sources of danger or the disabling of integrated safety devices.

Apart from the safety instructions listed in this manual, the occupational safety precautions and accident prevention measures appropriate to the situation in question must also be observed.

Handling the devices

The following information must be observed while operating the devices to prevent any malfunctions or damage caused by improper handling:

WARNING!

The following application areas are expressly excluded for the KeTop without completing a special evaluation relating to the application and implementing the necessary measures in the installation relating to the operating conditions:

- Use in areas where there is a risk of explosion or fire
- Use in the mining industry
- Outdoor use

For these applications, special products designed for the specific environments are to be used!

ESD

The housing must not be opened, as the device is sensitive to electrostatic discharge.

Information

This product was developed for use in industrial areas and can cause radio interference if used in residential areas.

© KEBA 2021

Caution

Improper handling will destroy the device or the control system!

Turn off the supply voltage before inserting or removing devices. Otherwise, the devices can be destroyed or undefined signal states can lead to damage.

To protect the devices from damage during further transport or return transport, the original packaging must always be used for transport.

Caution

- Ensure that the handheld device is not set down on the operating side, which could cause operating elements to be mechanically damaged or unintentionally actuated.
- Never set the handheld device on unstable surfaces / shelves. It could fall down and be damaged as a result.
- Never mount/place the devices in the vicinity of heat sources or direct sunlight.
- Avoid exposing the devices to mechanical shocks, excessive dust, humidity or to strong magnetic fields.
- Do not lay the cables over sharp edges to avoid damaging the cable sheath.
- Make sure that no foreign objects or liquids can penetrate the device. At regular intervals and especially after severe shocks (e.g. a fall), check the protective covers on the device, ensure all housing screws are firmly tightened and check the housing or cable feed through for damage.
- If the device indicates an error, remove it from operation and send it, including a detailed error description, to your supplier or the relevant after-sales service office.
- Place/hang the device, if present, in the intended charging station when you are not using it.
- The handheld device must not be operated with pointed or sharp objects (e.g., screwdrivers, etc.) because this may destroy the device. Operate the device with a finger or with a touch pen.
- The connection slot can only be opened when the device is switched off. Otherwise, components can be destroyed or undefined signal states can occur.

KEBA © KEBA 2021

2.3 Personnel safety instructions

WARNING!

Risk of electric shock to persons!

- Charge the handheld device and/or supply the base station exclusively from power sources that have a safety or protective extra-low voltage (e.g. SELV or PELV according to EN 61010-2-201).
- Connecting a SELV voltage source can, depending on the variant, turn it into a PELV voltage source.
- Only connect voltages and electric circuits that have a safe disconnect for hazardous voltages (e.g. with sufficient isolation and electric strength) to connections, terminals and interfaces with a rated voltage of up to 50 V.

CAUTION!

Fire hazard in the event of component failure!

Provide suitable fuses for the 24 V DC power supply of the device when supplying the base station with power. For this purpose, a UL 248 approved fuse must be used at max. 3.15 A.

Only charge the handheld device with the charging devices recommended by KEBA and with the intended charging equipment (charging station and power adapter).

© KEBA 2021

WARNING!

- The machine manufacturer must ensure proper configuration of the system based on the risk assessment. The following safety aspects must be considered for this purpose, among other aspects:
  - Proper restriction of the work area (optional with operation area monitoring module)
  - Emergency stop concept necessary
  - Category and performance level sufficient for the respective application
- Personnel must have a view into the hazard area from the operating area where they are standing.
- The base station must not be installed in the hazard area of the machine. (See 5.7.1 Positioning the base station.)
- The devices may only be operated when they are in a flawless condition and in compliance with the operating instructions.
- If emergency stop devices are attached to wireless operating stations (e.g. wireless programming devices), then at least one emergency stop device must always be available on the machine.
- Handheld terminals that are not used (not connected) must be placed in storage so that there is no risk of them being confused with a connected handheld terminal.
- No persons must be in the hazard area of the machine while a handheld terminal is being paired to / unpaired from of the base station.
- The operator must have the required level of training and know and understand the specific details of what constitutes the intended use in accordance with the operating instructions.
- The safety notes and information in the subsequent chapters must always be observed.

KEBA © KEBA 2021

CAUTION!

Danger to persons due to fire hazard or chemical burn!

The battery must only be used for the intended use.

The battery must not be dismantled, opened or crushed.

The battery must not be short-circuited.

Charging station and cables must show no signs of damage.

In case of battery leakage, the fluid must not come into contact with the skin or eyes. In case of contact, wash the affected area with plenty of water and see a doctor.

Do not subject the battery to mechanical shock, crush, impact, or puncture.

The battery must not be exposed to fire or heat.

The battery must not be exposed to dirt or humidity.

The battery must not be disposed as residual waste but must be recycled according to national and local regulations. Before disposal, the battery must be completely discharged or the contacts must be isolated with adhesive tape.

The battery may only be replaced by a battery purchased from KEBA. Use of another battery may present a risk of fire or explosion.

Caution

Battery failure due to improper handling!

The battery must be charged before first use.

- Avoid direct exposure to sunlight.
- Store the battery in a cool, dry, and well-ventilated area.
- Store the battery in an environment free of dust and corrosive gases.
- Do not leave the battery in the charger for more than 24 hours.
- The battery must be charged completely before first use.
- The battery must only be stored in its original packaging. Avoid containers in which loose metallic parts could cause short circuits.
- Do not store the unpacked battery in containers in which loose metallic parts could cause short circuits.
- Do not store a battery longer than 1 month in a discharged state.

© KEBA 2021

2.4 ESD information

Electronic component are generally put at risk by electro-static discharges (**E**lectro **S**tatic **D**ischarge). An electro-static charge can occur during any activity involving movement. ESD can occur with any touch.

Most discharges are so low that they are not noticeable. However, they can nevertheless put unprotected electronic components at risk or even destroy them. Therefore, any handling with open electronics is only permissible with the application of effective ESD protection.

When handling **open** electronics, please follow the following ESD measures:

- Only touch open electronics if this is absolutely necessary.
- Wear a conductive ESD wristband.
- Use conductive mats.
- Establish a conductive connection between device/system, mat, wristband, and grounding connection.
- Cotton work clothes are preferred over synthetic fiber materials.
- Keep work area free of highly isolating materials (e.g. Styrofoam, plastics, nylon, ...).
- Use ESD protection even for defective modules.

Always keep the devices in their original packaging and only remove the packaging immediately before installation.

Avoid, for modules which are mounted in an enclosure, direct contact with any accessible electronic components, such as non-equipped terminals.

KEBA © KEBA 2021

3 System overview

The Safe Wireless system consists of one or more wireless handheld devices and one or more base stations. The data is transmitted between the handheld device and base station using radio connections. The radio connections to the base station consist of a channel for transmitting sensitive information, also called "secure connection," (e.g. for the illuminated emergency stop) via Bluetooth and a channel for transmitting non-sensitive information, also called "unsecure connection," via Wi-Fi. Depending on the configuration, the Wi-Fi of the base station or the Wi-Fi of the hall network for the unsecure connection can be used. At all times, the secure connection is established between exactly one handheld device and one base station.

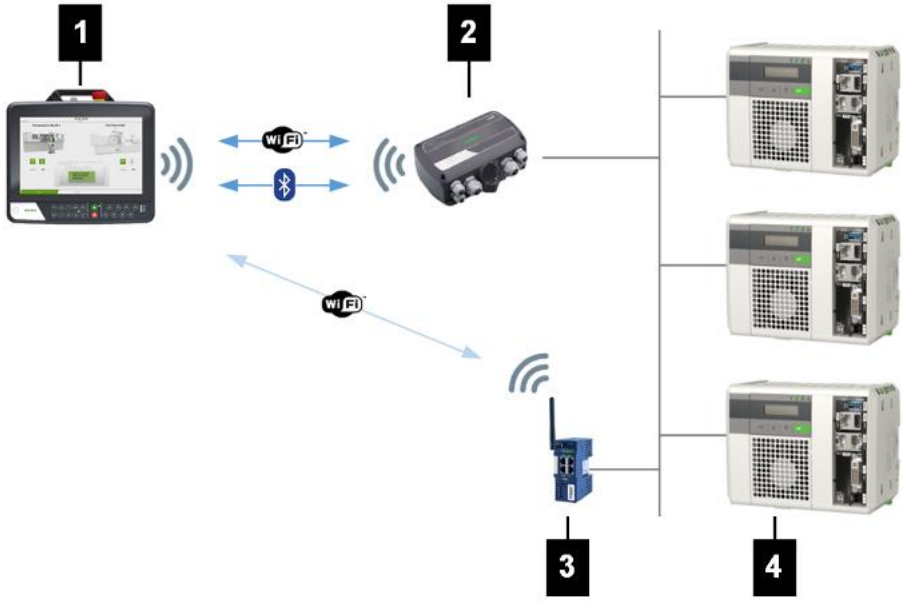


Fig. 3-3: System structure

1 ... Handheld device	2 ... Base station
3 ... Hall network	4 ... Controls

Operation with secure connection

To establish a secure connection, one handheld device must explicitly be paired with exactly one base station. Because the connection is a "point to point" connection, there is always exactly one handheld device connected to exactly one base station. The set-up of the base station must ensure that the handheld device can only be paired where the user can visualize the danger zone.

10 systems (handheld device with base station) can be operated in parallel over an area of 400 m².

The security settings on the handheld device are only functional if there is a secure connection (via pairing) to the base station.

© KEBA 2021

Depending on the configuration, non-sensitive data can be transmitted via the Wi-Fi of the base station or via the Wi-Fi of the hall network.

After terminating the operations, the handheld device must be unpaired from the base station. Then, a new connection to any available base station can be established.

WARNING!

If there is more than one base station on one and the same machine, it must be ensured that only one combination (base station/handheld device) acts on the machine. In some cases, the base stations must be locked out of each other ("Single Point of Control"). This must be implemented in the higher-level safety concept.

Operation with "unsecure connection" (functional connection)

When operating the device with an "unsecure connection", the handheld device is only connected to the Wi-Fi of the hall network. The security settings on the handheld device are not available. There is only an option to exchange functional data. This exchange is done using the configured Wi-Fi connection in the hall network. It is not possible to transmit secure data. Pairing to / unpairing from a base station is not necessary for this operation case.

3.1 Operation area monitoring (= OAM; optional)

Information

If desired, operation area monitoring can also be implemented later by KEBA.

Operation area monitoring is available to ensure that no dangerous actions of the machine or of machine parts can be triggered outside the visible part of the hazard area. Operation area monitoring also offers the advantage of reducing the probability of connection interruptions. As long as the operator is in the configured operation area, the user cannot perceive the operation area monitoring. Tactile and visual measures (vibration in the handheld device and pulsation of the illuminated emergency stop) let the operator know when he or she has reached the boundary of the operation area and is now in the tolerance range. If the operator then continues moving into the infringement area, these measures become more frequent. If the user moves into the effective range, the frequency is reduced. This chapter describes the availability of the safety functions in these three zones.

KEBA © KEBA 2021

Information

When operation area monitoring is active, observe the additional notes about pairing/unpairing (see 11 Pairing to base station).

WARNING!

Risk of injury due to hazard areas outside the field of vision

The operation area monitoring module measures the distance between the handheld device and base station. The system's operation area must be designed in such a way that it is possible to see into the hazard area within this distance. Even in the tolerance range, it must be possible to see into the hazard areas.

The operation area monitoring module distance measurement must be validated during commissioning or when the work area is changed and must be checked for proper function periodically (every month) (see 10.1 Validating the distance measurement).

The operation area monitoring covers a hemisphere in front of the base station. Consequently, for the efficiency and accuracy of the system it is very important to have the base station positioned properly (see 5.7.1 Positioning the base station).

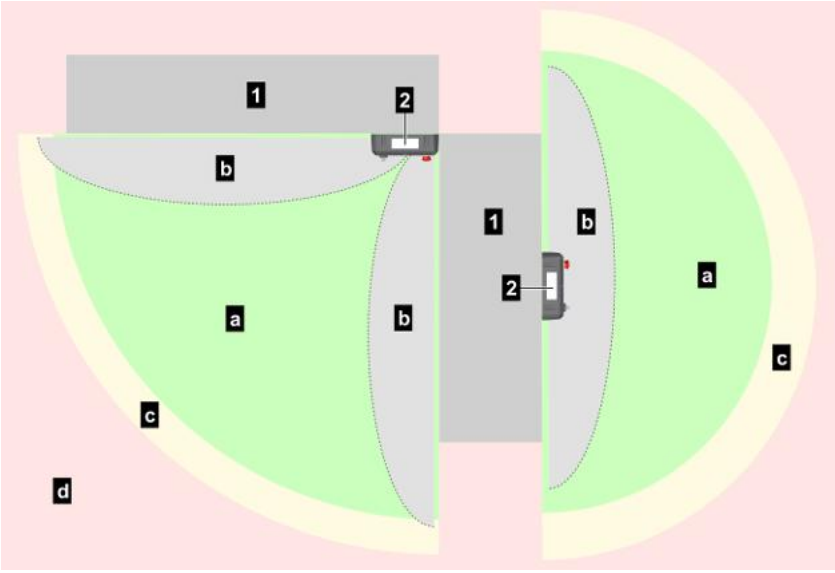


Fig. 3-4: Example of installation floor plan

1 ... Machine	2 ... Base station
a ... Configured operation area	b ... Designated work area
c ... Tolerance range	d ... Area of infringement

© KEBA 2021

The maximum configurable operation area is 20 m and can be configured on the base station by means of DIP switches (see 8.3 Operation area configuration (safety-related)).

The operation area monitoring communications channel is determined automatically in the device configuration and may be configured on the handheld device (see 8.4.5 Network). Upon successful configuration, the additional wireless connection is established automatically and starts the monitoring.

Over an area of 500 m^2, up to 5 connections (handheld device and base station) with operation area monitoring can be operated in parallel.

Zones of operation area monitoring

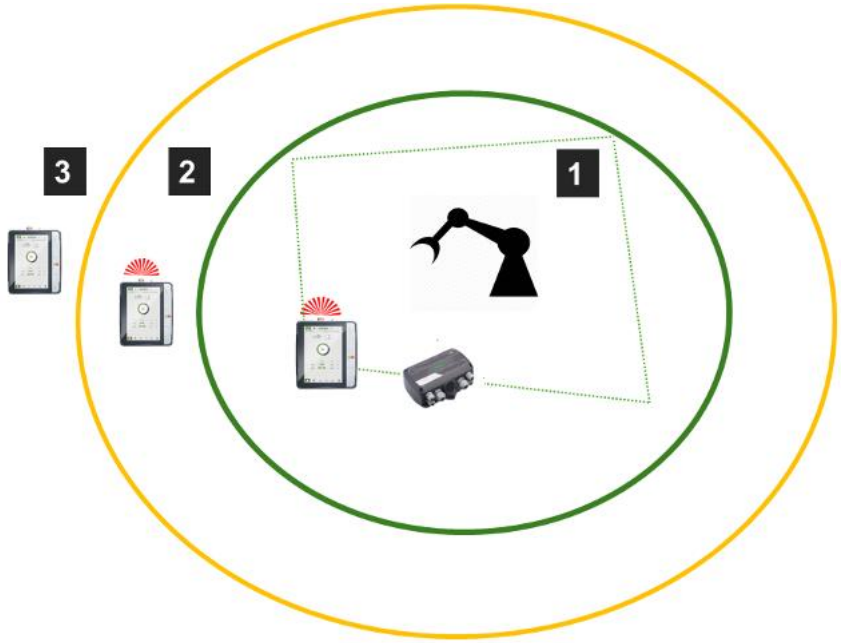


Fig. 3-5: Zones of operation area monitoring

1 ... operation area	2 ... Tolerance range
3 ... Area of infringement	

The solid green line represents the boundary of the work area, which is configured as the operation area. The farthest point in the work area defines the operation area (comparable to the cable length for wired devices).

The yellow line represents the tolerance range. The tolerance value is set to 3 m by default and is not configurable. This value is applied in addition to the radius.

To switch from the tolerance range back into the operation area, it is necessary to move 2 m into the defined work area.

KEBA © KEBA 2021

Information

The operation area monitoring distance measurement is most accurate when the back of the handheld device is facing the front of the base station. If the handheld device is shielded (e.g. by the body of the operator), this can cause the measuring system to output falsely high distance values, which can result in the machine coming to an undesired standstill.

If the handheld device is not in a hemispherical area in front of the base station, this can cause the measuring system to output falsely high distance values, which can result in the machine coming to an undesired standstill.

If the handheld device is aligned as described here and a minimum distance of 3 m is maintained, this system achieves a measuring tolerance of +/- 1 m. Even if the alignment is not optimal, the measuring tolerance of - 1 m is not undershot.

Operation area

In the operation area, the full range of functions is ensured when there is a connection. The emergency stop is illuminated and functional. The enabling switch is also functional.

Tolerance range

When someone enters the tolerance range, this is indicated by vibrations in the handheld device and optical signals. The emergency stop switch is no longer uniformly illuminated in the tolerance range, but rather the light pulsates. The emergency stop is still functional, however.

When the enabling switch is pressed, the output is removed after approx. 10 sec. (not adjustable). If the enabling switch is not pressed when the tolerance range is entered, enabling is no longer possible. The operation area is the only area where enabling is possible when the enabling switch is released and pressed again.

Area of infringement

When someone enters the infringement area (i.e. exits the tolerance range), this is indicated right away by strong vibrations and optical signals.

The emergency stop function is triggered after about 3 sec. (not adjustable) and the LED in the emergency stop switch on the handheld device is deactivated. The machine enters a safe state.

If the enabling switch is pressed, this is deactivated immediately when someone enters the infringement area. An enabling switch that has not been actuated can no longer be activated.

© KEBA 2021

Compatibility

KeTop T15xWL	KeTop CB4xx	Establishing a connection
With operation area monitoring	With operation area monitoring	Possible
Without operation area monitoring	Without operation area monitoring	Possible
With operation area monitoring	Without operation area monitoring	Possible
Without operation area monitoring	With operation area monitoring	Not possible

3.2 Order overview

Handheld device

	KeTop	T	150	WL	-	R	1	0	-	E	N	0	-	W10E
Product group	KeTop													
Version specification														
• KEBA standard		T												
• Customer-specific (Customized)		C												
Format														
• Portrait			150											
• Landscape			155											
Wireless				WL										
Membrane keyboard														
• KEBA standard keyboard						D								
• KEBA robotics keypad						R								
• Customer-specific labeling of the KEBA standard keyboard						1								
• Customer-specific keyboard						2								
Passive operating elements mounted next to the E-Stop (not safety-related)							1							
Passive operating elements mounted on the front (not safety-related)								0						
Functional safety										E				
CPU / SSD memory														
• 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			
Options														
• Without operating area monitoring (OAM)												0		
• With OAM 1.0												1		
• With OAM 2.0												2		
Software specifications														W10E

Base station

KeTop CB410-EE1-xxx

	KeTop	CB4	1	0	-	E	E	1	-	xxx
Product group	KeTop									
Version		CB4								
Emergency stop/enabling switch outputs										
• Relay / semiconductor outputs			1							
• PROFIsafe			2							
• FSoE			3							
Base station installation type										
• Without cable outlet				0						
• With cable outlet				1						
Functional safety										
• Incl. emergency-stop button						E				
Passive operating element mounted next to the E-Stop (not safety-related)							E			
Configuration										
• Pairing/remote pairing outputs (PO/SPO)								0		
• PO/SPO + functional fast-response outputs (FRB)								1		
• PO/SPO + FRB + operating area monitoring (OAM 1.0)								2		
• PO/SPO + operating area monitoring (OAM 1.0)								3		
• PO/SPO + FRB + operating area monitoring (OAM 2.0)								4		

© KEBA 2021

	KeTop	CB4	1	0	-	E	E	1	-	xxx
● PO/SPO + operating area monitoring (OAM 2.0)								5		
Customer-specific										
● KEBA										0
● Customer										xxx

KEBA © KEBA 2021

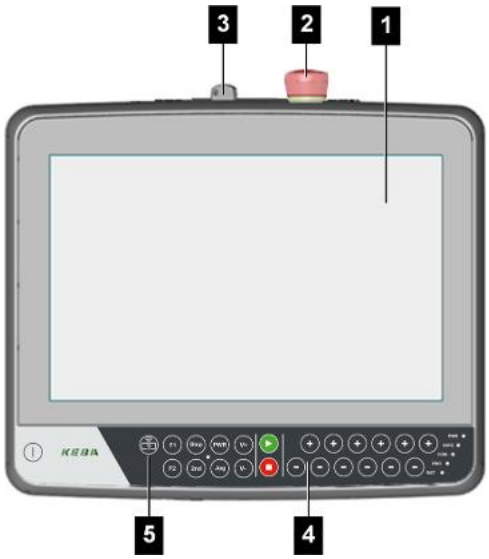
4 Description of the handheld devices

The handheld devices are portable operating and display devices with a robust design. All tasks can be handled on the color display using the graphical interface. The touchscreen enables intuitive operation. The delivered charging station can be used to charge and store the handheld devices.

With optional controls and control elements, the devices can be easily adapted to the particular application.

The machine manufacturer is responsible for selecting a handheld device that is suitable for the machine and designing any possible additional options that must be implemented in accordance with the legally required hazard and risk evaluation.

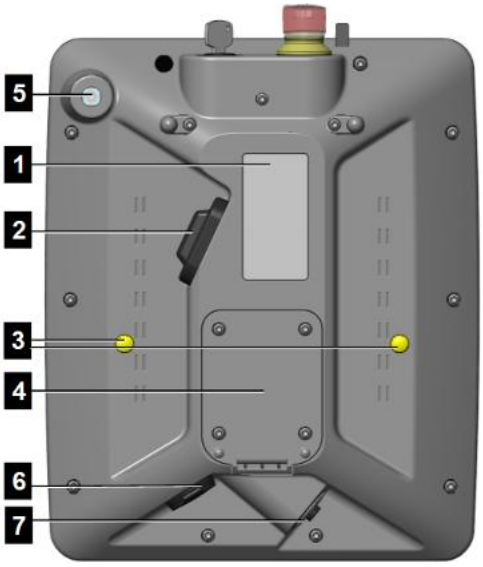
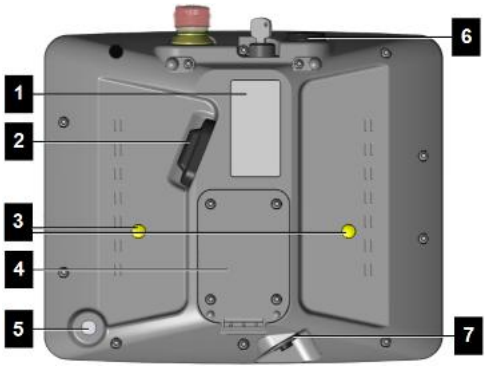
4.1 Front view

T150WL	T155WL
	

1 ...	TFT display with projective capacitive multi-touch screen	2 ...	Illuminated emergency-stop
3 ...	Slot for options	4 ...	Membrane keyboard
5 ...	"Ident" button		

© KEBA 2021

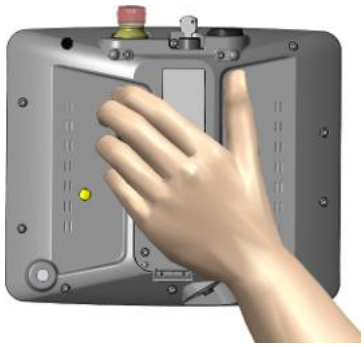
4.2 Rear view

T150WL	T155WL
	

1 ...	Serial type plate	2 ...	Enabling switch
3 ...	Charging contacts	4 ...	Slot cover
5 ...	Camera (optional)	6 ...	USB port
7 ...	External power supply (DC socket suitable for DC barrel connector 5.5/2.1)		

4.3 Handling

The handheld terminal is held with the left hand. Here, the enabling switch can be operated by hand. The touchscreen and the keyboard can then be operated with the other hand.

T150WL	T155WL
	

KEBA © KEBA 2021

4.4 Type plate

The type plate is located on the rear side of the handheld device. It contains product-specific information as well as technical data and regulatory markings.

The following sections show the type plates for the respective device variants.

4.4.1 Type plate Celeron N2807

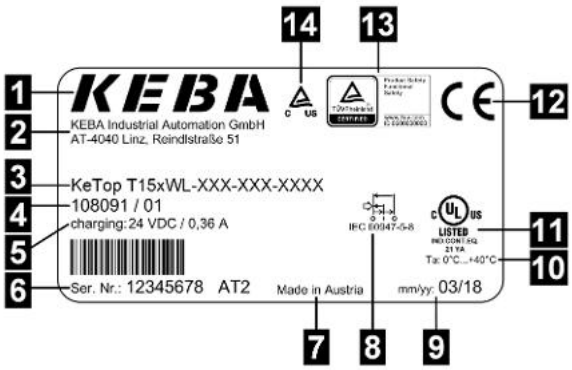


Fig. 4-6: Type plate

1 ... Manufacturer	2 ... Manufacturer's address
3 ... Product designation	4 ... Material- / revision number
5 ... Technical data (voltage / current)	6 ... Serial number
7 ... Country of manufacture	8 ... Standard and icon for 3-stage enabling device
9 ... Production date	10 ... Ambient temperature
11 ... UL marking	12 ... CE marking of conformity
13 ... TÜV marking	14 ... cTÜVus marking

© KEBA 2021

4.4.2 Type plate Intel Atom x6211

KeTop with operating area monitoring (OAM)

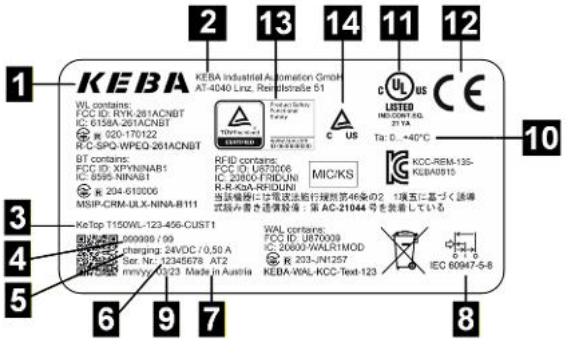


Fig. 4-7: Type plate KeTop with OAM

1 ... Manufacturer	2 ... Manufacturer's address
3 ... Product designation	4 ... Material / revision number
5 ... Technical data (voltage / current)	6 ... Serial number
7 ... Country of manufacture	8 ... Standard and icon 3-stage enabling device
9 ... Production date	10 ... Ambient temperature
11 ... UL marking	12 ... CE marking of conformity
13 ... TÜV marking	14 ... cTÜVus marking

KeTop without operating area monitoring (OAM)

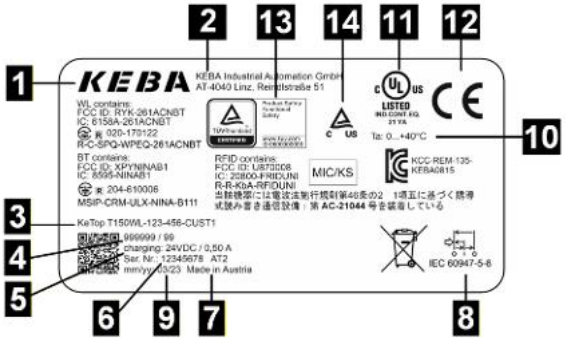


Fig. 4-8: Type plate KeTop without OAM

1 ... Manufacturer	2 ... Manufacturer's address
3 ... Product designation	4 ... Material / revision number
5 ... Technical data (voltage / current)	6 ... Serial number
7 ... Country of manufacture	8 ... Standard and icon 3-stage enabling device
9 ... Production date	10 ... Ambient temperature
11 ... UL marking	12 ... CE marking of conformity
13 ... TÜV marking	14 ... cTÜVus marking

KEBA © KEBA 2021

4.5 Display and operating elements

- Membrane keys with tactile feedback
- Status LEDs
- Capacitive multi-touch screen, with finger operation
- Backlit color LED display

Caution

Damage to the keypad for improper handling!

- The keypad may not be operated with sharp, metallic objects or with ball point pens or pencils.
- Too much force when pressing can damage the keys.

4.5.1 Standard keypad

KeTop T150WL

Variant of the membrane keypad, equipped with 22 keys and 5 status LEDs.

Fig. 4-9: Standard keypad, front side

KeTop T155WL

Variant of the membrane keypad, equipped with 22 keys and 5 status LEDs.

© KEBA 2021

Fig. 4-10: Standard keypad, front side

Variant of the membrane keypad with recess for optional installation element (e.g. handwheel), equipped with 22 keys and 5 status LEDs.

Fig. 4-11: Standard keypad with recess, front side

4.5.2 Robotics keypad

KeTop T150WL

Membrane keypad, equipped with 24 keys and 5 status LEDs.

Information

The handheld device T150WL is equipped with the robotics keypad as standard.

Fig. 4-12: Robotics keypad, front side

KEBA © KEBA 2021

Variant of the membrane keypad with recess for optional installation element (e.g. handwheel), equipped with 24 keys and 5 status LEDs.

Fig. 4-13: Robotics keypad with recess, front side

KeTop T155WL

Membrane keypad, equipped with 24 keys and 5 status LEDs.

Fig. 4-14: Robotics keypad, front side

Variant of the membrane keypad with recess for optional installation element (e.g. handwheel), equipped with 24 keys and 5 status LEDs.

Fig. 4-15: Robotics keypad with recess, front side

4.5.3 CNC keypad

Variant of the membrane keypad, equipped with 20 keys and 5 status LEDs.

© KEBA 2021

Fig. 4-16: CNC kaypad, front side

4.5.4 Status LEDs

The mobile handheld device is equipped with the following LEDs:

PWR (power supply)

LED	Description
Dark	No power supply (e.g. battery dead)
Flashing green	Power supply available, device switched off
Green	Supply voltage present, device ready for operation

SAFE (secure connection)

LED	Description
Dark	Device is not paired with a base station
Green	Device is continuously paired with a base station

Information

A lighted SAFE LED indicates that the handheld terminal is safely connected ("paired") to a base station, even if there is no active wireless connection.

RNG (operation area monitoring)

LED	Description
Dark	No operation area monitoring configured or available
Green	Operation area monitoring active

COM (WLAN)

LED	Description
Dark	No Wi-Fi connection established
Green	Existing Wi-Fi connection

BAT (battery)

LED	Description
Dark	Battery completely charged or device in operation
Green	Battery of the device being charged

KEBA © KEBA 2021

LED	Description
Flashing green	Battery cannot be charged. No battery available / Battery damaged / Undervoltage / Temperature >45°C

4.5.5 "Ident" button

The "Ident" button is used to identify which base station the ready-to-operate handheld device is paired with.

Holding the "Ident" button (for > 3 sec) opens a dialog indicating whether the handheld device is paired with a base station and/or which base station it is paired with. If the button is only pressed briefly, the LED bar on the paired base station displays a flashing pattern.

4.5.6 Touchscreen

A projective-capacitive multi-touch screen is used.

Caution

Material damage due to overstressing the screen!

A burn-in effect can occur with LC displays when a static image or a constantly repeated graphic is displayed over a longer period of time.

The burn-in effect can and should be prevented by regularly changing the displayed image, using a screen saver and reducing the brightness and contrast of the display.

Operation

The touchscreen may be operated with one or more fingers (with or without glove). For long durability of the touch screen, the following points should be observed:

Caution

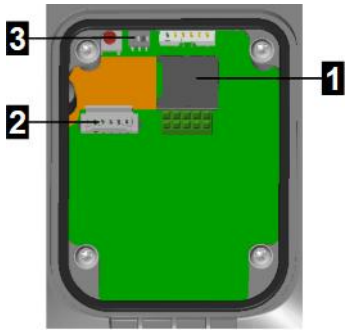
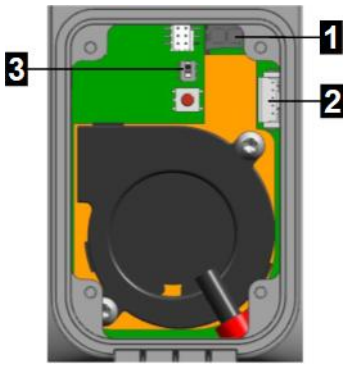
Damage to the touch screen for improper handling!

- Use only a soft cloth with mild detergent (e.g. soapsuds) to clean the touch screen, see 13.1 Cleaning the touchscreen.
- When operating with gloves, ensure that no metal filings or sharp objects (sand, grinding paste, etc.) are embedded in the surface of the glove.
- The touch screen may not be operated with sharp, metallic objects or with ball point pens or pencils.
- The touch screen my not be exposed to continuous direct sunlight.

© KEBA 2021

4.6 Connection and wiring

4.6.1 Cable entrance area

T150WL	T155WL
	

1 ...	Micro SD card slot	2 ...	Pin strip - battery plug
3 ...	DIP switch (8.7 Configure hibernation)		

4.6.2 Plugging in battery

When delivered, the battery is not connected and only 30% charged. The battery must be fully charged before use.

After opening the connection slot, the battery can be connected. Before opening the KeTop, please observe the following information:

Information

Information for opening the connection slot:

- Place the handheld device on a flat, clean and soft surface with the display facing down so that the handheld device or its operating elements are not damaged (e.g. ESD mat).
- Use a "Torx size 10" type screwdriver to open and close the connection slot.

Information

Information on changes in the connection slot:

- When connecting and disconnecting the battery plug, it must be ensured that you use your fingers to unplug the connector from its wires (do not use sharp objects to help with this process).

KEBA © KEBA 2021

Information

Information on closing the connection slot:

- The seal must be clean, undamaged and in the correct position.
- The cables must not be pinched.
- The connection duct cover must be screwed together again using all 4 screws (torque: 0.8 to 1.0 Nm). This is the only way to ensure the corresponding protection class.

4.6.3 Power supply

WARNING!

Please observe the safety-relevant information in chapter 2.3 Personnel safety instructions.

The handheld device is supplied with voltage by a battery. The battery can be charged either using the charging station or using an external power supply.

4.6.4 Illuminated emergency stop

The illuminated emergency stop has the same functionality as a red-yellow emergency stop. It is wired as a 2-circuit switch and the contacts are designed as N.C. The difference is that this emergency stop is recognizable as an emergency stop element only in the connected (i.e. operationally ready) state because of the illumination.

Emergency stop illuminated	Emergency stop not illuminated

The illuminated emergency stop switch works only if the handheld device is paired with a base station and (in the event that an optional operation area is configured) only if the device is located within the operation area.

The emergency stop on the handheld device corresponds to the requirements of EN ISO 13850. Based on the risk assessment for the machine, the operating principle of the emergency stop must be designed as a stop of Category 0 or Category 1 (see EN 60204-1). The wiring of the positively

© KEBA 2021

driven relay contacts at the base station must fulfill the specific category (in acc. with EN ISO 13849-1) that is defined based on the risk analysis of the machine (in acc. with EN ISO 12100:2010).

WARNING!

- An unlocking of the emergency stop system must not trigger an uncontrolled restart.
- The emergency stop is no substitution for safety systems.

WARNING!

- The illuminated emergency stop on the handheld device is not a replacement for the emergency stop that is to be directly attached to the machine.
- When an illuminated emergency stop switch is used, it must be visually checked at each pairing/unpairing and periodically (once per month) to make sure it is functioning properly and has sufficient brightness. In the event of insufficient brightness or failure of the illumination, the handheld device must be replaced.
- In the final application, direct sunlight on the illuminated emergency stop button must be avoided so that the illumination status is always recognizable. When working out a machine/system safety concept, take into account the lifetime of the lighting. In the course of determining the brightness of emergency stop lighting, 1500 LUX were used as a basis in accordance with the Workplace Ordinance.

WARNING!

If the handheld device is exposed to a lot of dirt or if it comes into contact with small foreign objects, ensure that the cavity of the emergency stop switch is always unobstructed to ensure that there are no negative effects on the switching element function.

Certain mechanical errors in the emergency stop can only be detected during operation. After heavy impact on the device (e.g. due to dropping), the emergency stop must be checked for functional integrity. In addition, the emergency stop must be tested once per month through actuation. During this test, perform a visual inspection for any potential mechanical damage and severe contamination or possible functional impairment due to foreign objects.

Information

A defective LED in the emergency stop switch is indicated by the LED status bar at the base station and leads immediately to a safe state.

KEBA © KEBA 2021

4.6.5 Enabling switch

The KeTop is equipped with one enabling switch. The enabling switch consists of a 3-position operating element. An essential feature are the two-channel circuits and the forced opening according to EN 60947-1 and EN 60947-2 to the third switch position.

4.6.5.1 Requirements for enabling control device outputs and electronics

WARNING!

Output-side short-circuits cannot be detected by the enabling electronics. Using a suitable monitoring device (see chapter "Connection example with monitoring device"), a short circuit can be detected.

Information

Internally, the enabling electronics run cyclical tests for short-circuits and cross-circuits. For this self-test, the enable signal is taken away for the duration of the test impulse (max. 1 ms).
Faults in the enabling electronics are detected and lead to removing the enable signal at the output.

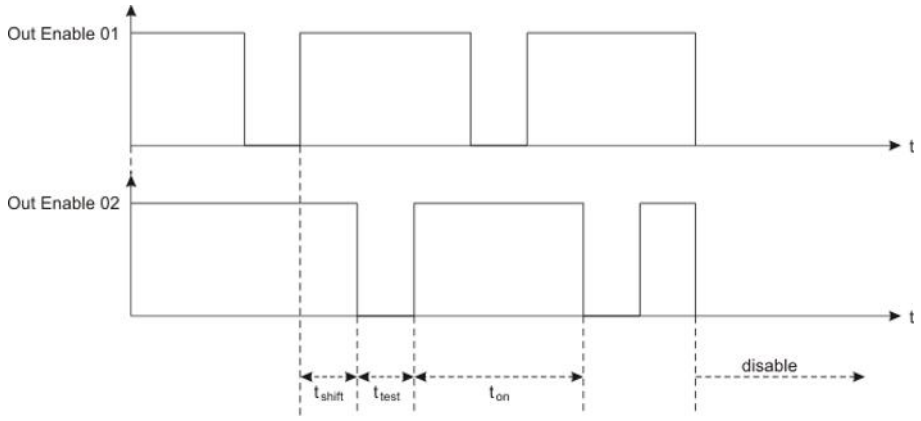


Fig. 4-17: Enabling electronics - Check for short-circuit and cross-circuit

Timing and request

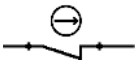
- t_{test}: ≤ 1 ms
- t_{on}: > 400 ms, ≤ 1000 ms

4.6.5.2 Functionality

The enabling switch can occupy three different switch positions:

Switch position	Function	Enabling switch	Switch contact
1	Zero position	is not operated	Off (opened)
2	Enabling function	is operated	On (closed)

© KEBA 2021

Switch position	Function	Enabling switch	Switch contact
3	Panic	is fully pressed	Off (opened) 

Pursuant to EN 60204-1, the enabling switch must be implemented in a manner that for the position 2 (off function of the switch - the operating element is not pressed) and position 3 (off function - the operating element is fully pressed to the "panic position") at least one of the stop categories 0, 1 or 2 is initiated.

For calculation of the PL of the enabling safety function, the safety-related indexes (PL and PFH_D values) of the components involved must be included in the calculation. Details for the calculation of the PL for the entire safety function can be found in EN ISO 13849-1 in Section 6.3 as well as Appendix H and Appendix I.

WARNING!

The enabling switch must be periodically tested (every month) by actuating the panic position. The panic position must be checked to verify that it is functioning properly.

Normal operation

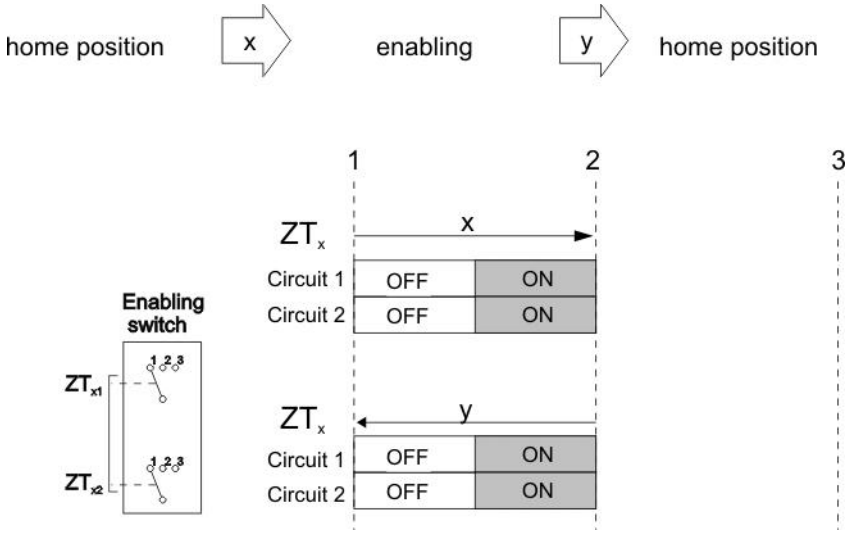


Fig. 4-18: Contact travel diagram for normal operation

Panic operation

The switching element for making a full press of the operating elements to panic position is mechanically designed so that the enable position is skipped over when released:

KEBA © KEBA 2021

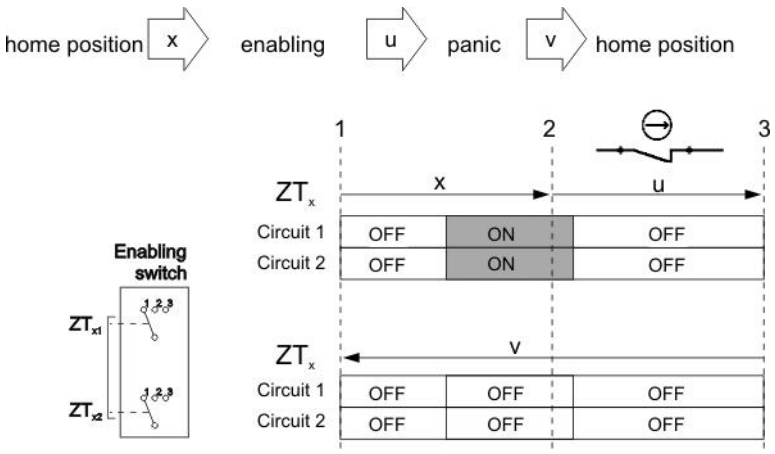


Fig. 4-19: Contact travel diagram for panic operation

Information

Enabling switches are always designed with two circuits for KeTop.

The Safe Wireless system achieves category 4 PL e in acc. with EN ISO 13849-1 and SIL3 in acc. with EN 62061 / EN 61508.

4.6.5.3 Foreseeable misuse of enabling switch

An unpermitted fixing of the enabling switches in the approval position by means of mechanical aids is to be seen as foreseeable misuse, which can be prevented.

The handheld device has the following integrated measures for this:

- If the enabling switch has already been pressed when the KeTop is switched on, then there is no enable signal output.
- During operation, if the enabling switch is held in the enable position for longer than 15 minutes, the enable signal is revoked until the enabling switch is released and operated again.

© KEBA 2021

WARNING!

- The enabling switch is only suitable as a protective function, if the person, who operates the enabling switch, notices an endangerment of a person in a timely manner and is then able to immediately take appropriate measures to avoid hazards. A reduced speed of the movement may be required as an additional measure. The permissible speed must be determined based on a risk assessment.
- Solely with an enabling switch it is not permitted to initiate any commands for hazard triggering conditions. A second, intentional start command is required in this case (button on the handheld terminal).
- Only the person, who has activated the enabling switch, is allowed to be present in the hazardous area.
- For additional information about the enabling switch, the "Safety of machines" chapter must always be observed.

4.6.6 USB port

Information

The USB interface is not designed as an operational interface for ongoing operations. It is used exclusively in the service and startup event for connecting USB devices.

Connecting a USB component

To connect, proceed as follows:

1) Open the protective dust cap (optional).
2) Insert the USB component so that it engages.

The USB component is recognized and displayed by the operating system.

Removing a USB component

Information

If there is an ongoing process of saving to the USB component, it cannot be disconnected during the saving process! This may otherwise result in loss of data.

To disconnect, proceed as follows:

1) Pull out the USB component.
2) Press on the protective dust cap firmly (optional).

KEBA © KEBA 2021

5 CB41x base station

The CB41x is the standard version of the base station. The CB41x may be used only in the configuration with KEBA wireless handheld devices with an illuminated emergency stop switch.

An emergency stop switch is provided on the base station as a safety function. The safety electronics of the emergency stop bypassing is designed with double circuits and facilitates implementation up to category 4 PL e in accordance with EN ISO 13849-1 or SIL 3 in accordance with EN 62061 / EN 61508.

At the time of delivery, the rear wall of the base station is not bolted to the rest of the box. A rear wall for the base station, which enables wiring on the back side, is available as an accessory (see 17.7 Rear wall for cable installation on the back side (only for CB41x)).

5.1 Front view

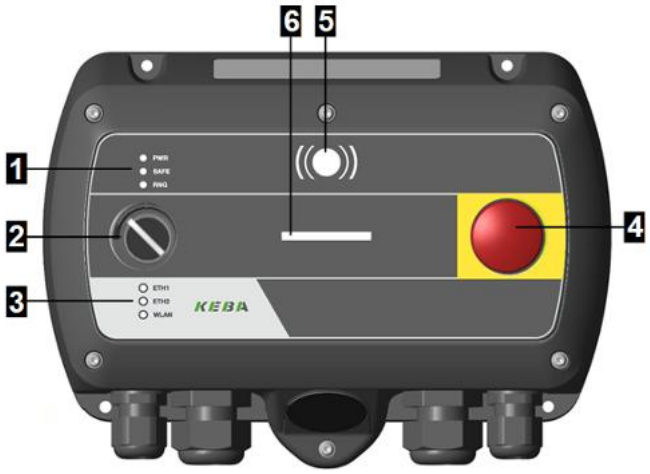


Fig. 5-20: Front side including optional operating elements

1 ... Status LEDs (PWR, SAFE, RNG)	2 ... Directly wired key-operated switch (optional)
3 ... Connection LEDs (ETH1, ETH2, WLAN)	4 ... Emergency stop
5 ... RFID sensor	6 ... Status LED bar

© KEBA 2021

5.2 Rear view

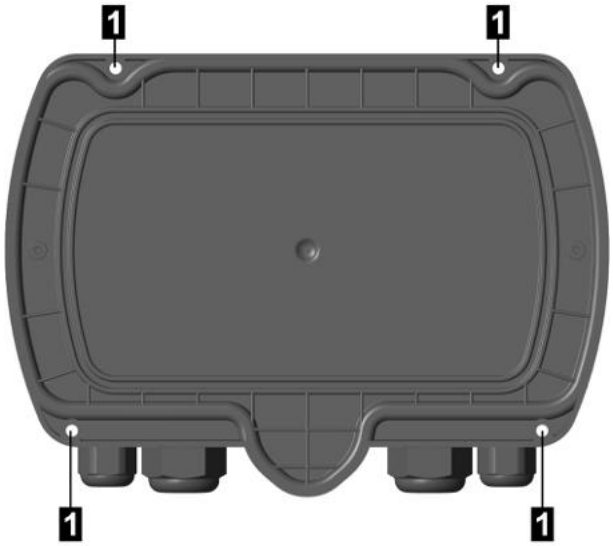


Fig. 5-21: Rear side

1 ... Drill holes	

5.3 Bottom view

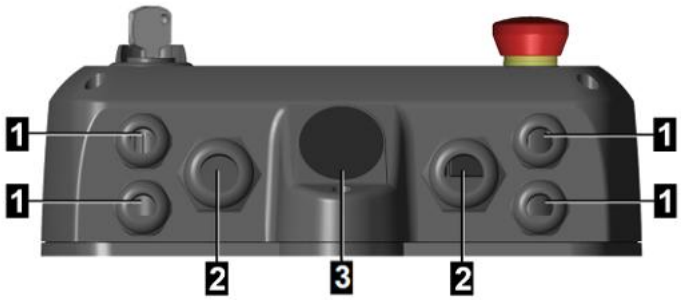


Fig. 5-22: Bottom

1 ... Standard cable outlets	2 ... Ethernet cable outlets
3 ... "Pairing Reset" button (capacitive)	

KEBA © KEBA 2021

5.4 Top view

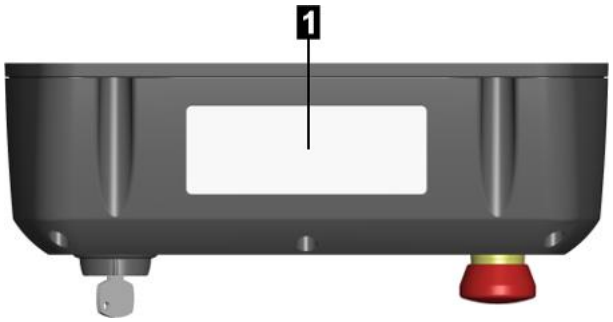


Fig. 5-23: Top

1 ... Type plate	

5.5 Type plate

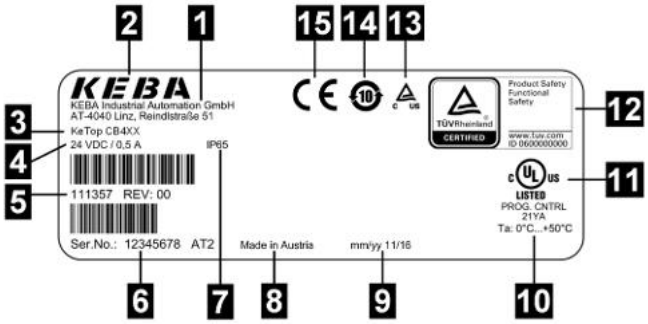


Fig. 5-24: Type plate

1 ... Manufacturer's address	2 ... Manufacturer
3 ... Product designation	4 ... Technical data (voltage / current)
5 ... Material and revision number	6 ... Serial number
7 ... Protection type	8 ... Country of manufacture
9 ... Production date	10 ... Ambient temperature
11 ... UL marking	12 ... TÜV marking
13 ... cTÜVus marking	14 ... China RoHS marking
15 ... CE marking of conformity	

5.6 Displays and operating elements

On the front side of the module, there are two LED groups and a status LED bar.

5.6.1 Status LEDs

The base station is equipped with the following LEDs:

© KEBA 2021

PWR (power supply)

LED	Description
Dark	No supply voltage, fault during startup
Green	Supply voltage present, device ready for operation

SAFE (secure connection)

LED	Description
Dark	No handheld device paired with the base station
Green	Handheld device continually paired

Information

A lighted SAFE LED indicates that the handheld terminal is safely connected ("paired") to a base station, even if there is no active wireless connection.

RNG (operation area monitoring)

LED	Description
Dark	No operation area monitoring configured or available
Green	Operation area monitoring active

5.6.2 Connection LEDs

ETH1 / ETH2

LED	Description
Dark	No Ethernet connection is available
Green	Active Ethernet connection (data transmission)

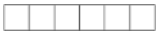
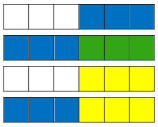
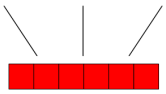
WLAN

LED	Description
Dark	WLAN module not available or not active
Green	WLAN module active

5.6.3 Status LED bar

Bar display	Signal column	Meaning
Green	Green	"Normal" operating state (see 9.3 Base station operating states)

KEBA © KEBA 2021

Bar display	Signal column	Meaning
White 	White	"Bridge active" operating state (see 9.3 Base station operating states)
Yellow LEDs going out successively	Yellow	"Pairing/Unpairing timer" operating state (see 9.3 Base station operating states)
Red	Red	"Estop" operating state (see 9.3 Base station operating states)
	White and blue Blue and green White and yellow Blue and yellow	"Remote Pairing" special operating state These displays are optionally shown during a remote pairing process and are used for unique identification of the base station.
Blue	Blue	Error state (see 12 Diagnosis)
Half red / half blue	Red and blue	Error state (see 12 Diagnosis)
Flashing half yellow / half red	Yellow and Red	Error state (see 12 Diagnosis)
Flashing red 	Red and White	Error state (see 12 Diagnosis)
Red chaser light	Red	Error state (see 12 Diagnosis)

5.6.4 "Pairing Reset" button

The "Pairing Reset" button is used for manually forcing the handheld device to unpair. To do so, the "Pairing Reset" button must be held for > 5 s.

This function is required if it is no longer possible for the handheld device to be unpaired from the base station on a regular basis (e.g. defect on the handheld device, handheld device physically too far away from base station, etc.). The function is available only if the base station no longer has any connection to the handheld device and is in the "Connection interrupted" state.

5.7 Mounting and installation instructions

WARNING!

The base station must not be installed in the hazard area of the machine.

© KEBA 2021

5.7.1 Positioning the base station

The base station makes it possible for the handheld device to access the radio network. Correct positioning of the base station enables fault-free operation to the greatest extent possible.

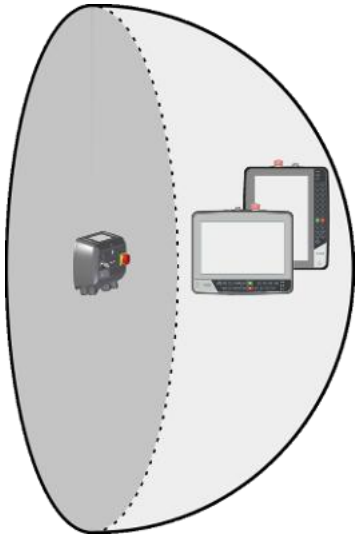


Fig. 5-25: Positioning the base station

The following points should be taken into account when selecting the position of the base station:

- The base station must be set up with a clear line of sight to the movement radius of the handheld device. The LED bar (or the signal column) must always be clearly visible from the hazard area.
- The base station should be installed as far away from large metal surfaces, glass surfaces or walls as possible.
- The base station must be installed in an unshielded area.
- The base stations themselves must be installed as far away from each other as possible. A minimum distance of 2 m must be maintained.
- The distance to the nearest Wi-Fi connection (access point) must be at least 4 m.
- The minimum distance between the base station and objects or structural surroundings is 1 m above and below and 0.5 to the left and right.
- The base station should be easy to reach with the handheld device, since the pairing process must happen within a distance of 0 to 2 m between the base station and the handheld device.

5.7.2 Drilling template for wall mounting

The rear wall of the base station can be used to mark the drill holes.

The fastening material is dependent on the construction material of the mounting surface on which the base station is being installed.

KEBA © KEBA 2021

We recommend mounting the rear wall using four M4 bolts with a maximum bolt head diameter of 9 mm. We recommend securing the bolts properly and with self-locking if the mounting surface is the wall of a control cabinet, for example.

5.7.3 Installing the base station

Remove housing

For the mounting and wiring of the base station, the housing must be removed from the rear wall. For this purpose, 6 PT30x10 screws must be removed from the front of the base station using a size 10 Torx key (see figure). The removed screws are required again for assembly.

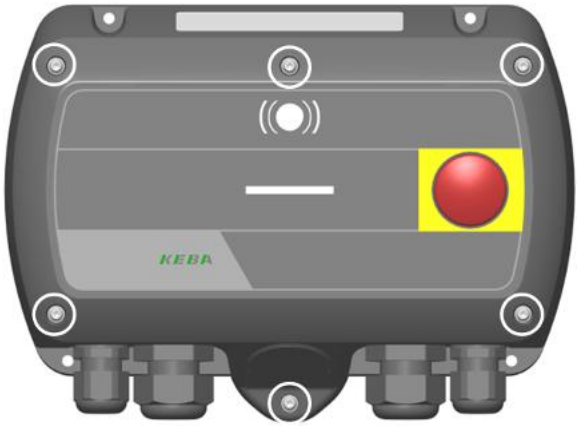


Fig. 5-26: Screws of the housing

Information

The base station is already wired between the housing and the rear wall. The connected cables can be disconnected during installation of the rear wall (see6.8.1 Internal wiring).

Installing the rear wall

Information

A rear wall is available as an accessory for the base station, which enables rear wiring (see Rear wall for cable installation on rear).

The rear wall of the base station must be installed before the base station can be installed on the mounting surface. To do this, proceed as follows:

1) Mark the drill holes using the rear wall of the base station.
2) Drill the holes.
3) Insert the dowels into the holes, if necessary.

© KEBA 2021

4) Install the rear wall on the wall using suitable screws, as shown in the following figure.

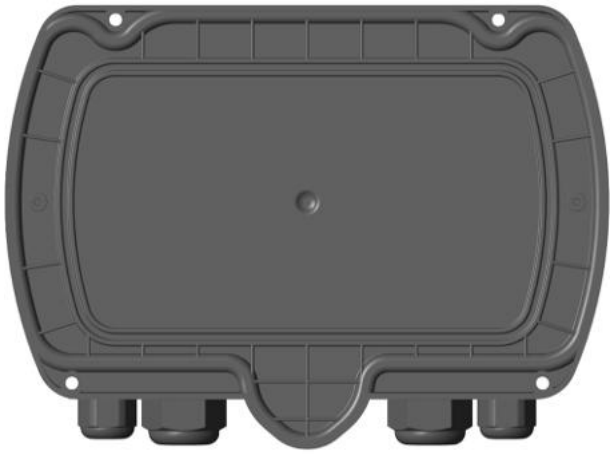


Fig. 5-27: Rear wall

The rear wall is now installed.

The wiring can then be executed, before the housing is closed (see Connections and wiring).

5.8 Connections and wiring

WARNING!

Faulty safety function!

Ensure that no pieces of wires, fillings or swarf fall into the device when you are drilling holes or connecting wires.

ESD

Note the ESD notes in chapter 2.4 ESD information.

Caution

The wiring of the CB4xx can only be executed by qualified electricians in accordance with the information provided.

The following connections are available and can be guided individually to the outside using the cable outlets.

KEBA © KEBA 2021

Information

Connection points, that are not numbered in the following illustration, must not be used.

CB410 base station connections

Fig. 5-28: CB410 base station connections

1 ... Terminal strip S1 / power supply	2 ... Ethernet interface
3 ... DIP switch (operation area configuration)	4 ... Terminal strip for "Pairing" / "Remote Pairing" outputs, "Fast Response" buttons (optional)
5 ... Terminal strip for "Fast Response" buttons (optional)	6 ... Terminal strip S2
7 ... Terminal strip for "Signal" for external LED display	

Wiring aid

The device can be turned over and attached to the installed rear wall for wiring.

For this purpose, the two upper holes on the front of the housing, used to bolt it in place, are attached to the two longer fastening pins on the rear wall.

© KEBA 2021

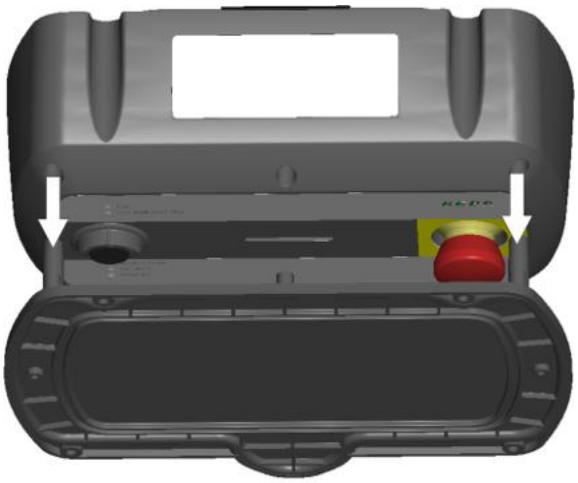


Fig. 5-29: Attaching to the rear wall

The cables are then fed through the corresponding cable outlets on the bottom of the device. These outlets have the following specifications:

Standard cable outlets

Clamping range (possible cable diameter):	4 to 8 mm
Degree of protection:	IP68
Size:	M16 x 1.5
Open-end wrench size:	SW19
Screw torque:	3 Nm

Ethernet cable outlets

Clamping range (possible cable diameter):	6 mm
Degree of protection:	IP68
Size:	M20 x 1.5
Max. diameter of RJ45 connector:	14.4 mm
Open-end wrench size:	SW27 (cap), SW24 (body)
Screw torque:	6 Nm

The screw connection must first be removed and pushed over the required cable so that the cables can be guided through the cable outlets. The seal ring, located in the cable outlet, must also be placed around Ethernet cables.

The cables can then be guided into the device, the screw connections can be tightened by hand again and the wiring can be implemented.

KEBA © KEBA 2021

Caution

Unused cable outlets must be sealed with the supplied blanking covers to ensure the protection class. To do this, remove the PG covers and install the blanking covers with the following torques (cross-slot size Z3):

- M16 × 1,5: 2 Nm
- M20 × 1,5: 2 Nm

A special rear wall is available as an accessory for any wiring via the rear (see 17.7 Rear wall for cable installation on the back side (only for CB41x)).

5.8.1 Terminal strip S1 / Power supply

The CB4xx is supplied with power at terminal S1. The signals for the enabling switch and emergency stop of the handheld device are also connected to the terminal.

WARNING!

Please observe the safety-relevant information in chapter 2.3 Personnel safety instructions.

If the base station is supplied with voltage, the PWR LED lights up green and the bar lights up white (= the emergency stop outputs of the base station are closed).

5.8.1.1 Pin assignment

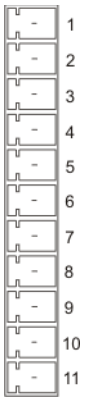


Fig. 5-30: Pin assignment

Pin no.	Signal designation	Description
1	N.C.	not connected
2	ZT2-	Approval control, circuit 2 negative
3	ZT1-	Approval control, circuit 1 negative

© KEBA 2021

Pin no.	Signal designation	Description
4	ZT2+	Approval control, circuit 2 positive
5	ZT1+	Approval control, circuit 1 positive
6	ES2	Emergency stop, circuit 2
7	ES1	Emergency stop, circuit 1
8	ES2	Emergency stop, circuit 2
9	ES1	Emergency stop, circuit 1
10	-	GND
11	+	24 V DC power supply

5.8.2 Terminal strip S2

Terminal strip S2 is directly wired and can be used for safety functions.

If the base station is equipped with an optional key-operated switch, the operating element signals are provided at terminal S2. The position of the key-operated switch is specified by combining the levels of two contacts (see 5.8.2.1 Pin assignment).

5.8.2.1 Pin assignment

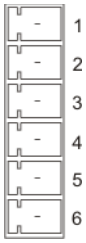
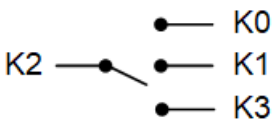


Fig. 5-31: Pin assignment

Pin No.	Signal designation	Description
1	GND	Grounding
2	n.a.	No use possible
3	K3	Key-operated switch contact: Position 3 (right switch position) 
4	K2	Key-operated switch contact: COMMON
5	K1	Key-operated switch contact: Position 2 (middle switch position)
6	K0	Key-operated switch contact: Position 1 (left switch position)

KEBA © KEBA 2021

5.8.3 "Signal" terminal strip

At the "Signal" terminal, a signal column can be connected.

The base station has been tested by KEBA with the following signal columns:

Manufacturer	Product designation
PATLITE	LR4-_02LJN
SPÄLTI	MES-502A-RYGBC(DC24V)

The use of these signal columns is recommended. Refer to the documentation from the manufacturer for more information.

Information

The "Signal" terminal strip may only be used to connect a signal column for displaying the operating and diagnostic states of the base station.

5.8.3.1 Pin assignment

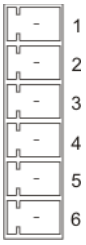


Fig. 5-32: Pin assignment

Pin No.	Signal designation	Description
1	24 V	24 V DC power supply
2	WH	Signal color: transparent/white
3	BU	Signal color: blue
4	Y/O	Signal color: yellow
5	GN	Signal color: green
6	RD	Signal color: red

5.8.4 "Pairing" / "Remote Pairing" outputs terminal strip

Via the combined use and plausibility check of the "Pairing" status output and the "Remote pairing" status output via an external safety controller, a safe operating mode switchover can be implemented. (For further information, see 11 Pairing to base station.)

© KEBA 2021

Possible states

PA1	PA2	Description
0 (open)	0 (open)	No device connected
1 (closed)	0 (open)	Device has been connected via pairing
0 (open)	1 (closed)	Device has been connected via remote pairing
1 (closed)	1 (closed)	There is a defect present

5.8.4.1 Pin assignment

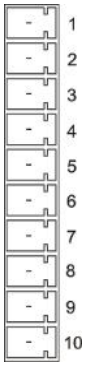


Fig. 5-33: Pin assignment

Pin No.	Signal designation	Description
1	PA1	Pairing output
2	PA2	Remote pairing output
3	PA1	Pairing output
4	PA2	Remote pairing output

5.8.5 Terminal strips for fast response buttons

The functional fast response buttons can be used to link buttons on the handheld device directly to the outputs of the base station. When a button is pressed on the handheld device, this is immediately applied to the linked output of the base station. This results in a shorter response time. (For configuration, see 8.4.1 Base station.)

KEBA © KEBA 2021

5.8.5.1 Pin assignment

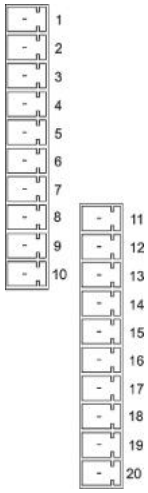


Fig. 5-34: Pin assignment

Pin No.	Signal designation	Description
5	GND	Ground
6	14	D14
7	13	D13
8	12	D12
9	11	D11
10	10	D10

Pin No.	Signal designation	Description
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

The device provides 2 Ethernet interfaces. They are provided to connect devices with which the handheld device should communicate. The interfaces can be fed through the cable outlets to the outside.

© KEBA 2021

5.8.6.1 Pin assignment

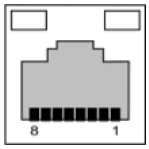


Fig. 5-35: RJ45 plug socket

Pin no.	Signal designation		Input / Output
1	Tr. Data+	Transmit Data +	Output
2	Tr. Data-	Transmit Data -	Output
3	Re. Data+	Receive Data +	Input
4	n.c.	n.c.	---
5	n.c.	n.c.	---
6	Re. Data-	Receive Data -	Input
7	n.c.	n.c.	---
8	n.c.	n.c.	---

5.8.7 Changes to the wiring

Information

Information about changes to the wiring:

- When disconnecting plug connections, be sure to use your fingers to unplug the connector from its wires (do not use sharp objects to help with this process).
- When disconnecting the RJ45 connectors, it must be ensured that the locking lever is activated during the process.

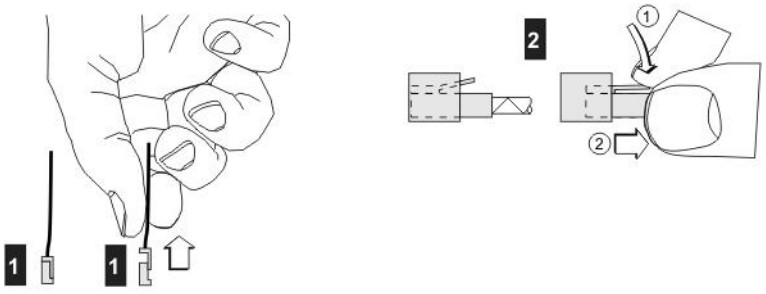


Fig. 5-36: Disconnecting the main plug and RJ-45 connector

1 ... Main plug	2 ... RJ45 connectors

KEBA © KEBA 2021

5.8.8 Closing the base station

The housing must be removed from the rear wall and turned over to close the base station. The housing can then be placed on the rear wall and secured using 6 PT30x10 screws (required tool - Torx size 10) as shown in the diagram. The screws are included in the scope of delivery.

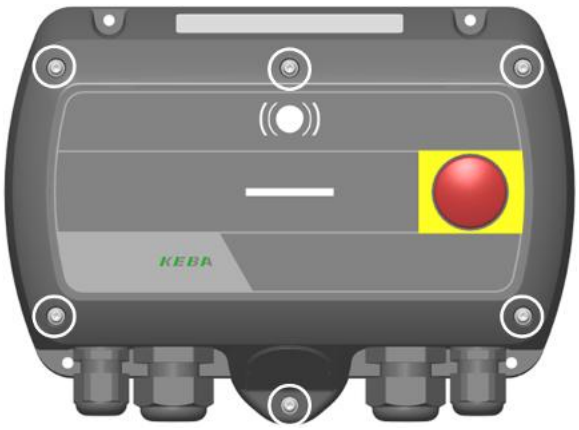


Fig. 5-37: Screws for closing

Information

Information on closing the base station:

- The seal must be clean, undamaged and in the correct position.
- No cables must be trapped.
- The base station must be screwed together again using all PT30x10 screws (torque: 0.85 Nm - 1.15 Nm). This is the only way to ensure the corresponding protection class.

The base station is ready for operation.

5.8.9 Emergency stop

The base station is equipped with an emergency stop.

WARNING!

Non-functional emergency stop systems can have fatal consequences! The red-yellow designated emergency stop must be operative at all times and in all operating modes of a machine or system.

© KEBA 2021

WARNING!

The emergency stop on the non-connected handheld device does not replace the emergency stop on the machine. A fixed, hardwired emergency stop must always be available on the machine.

5.8.10 Connection example of the enabling function with monitoring device (PILZ PNOZ s3)

WARNING!

A suitable monitoring device must be used for detecting short circuits and cross faults in the connection line.

The following example should serve as an aid for implementing this in the application.

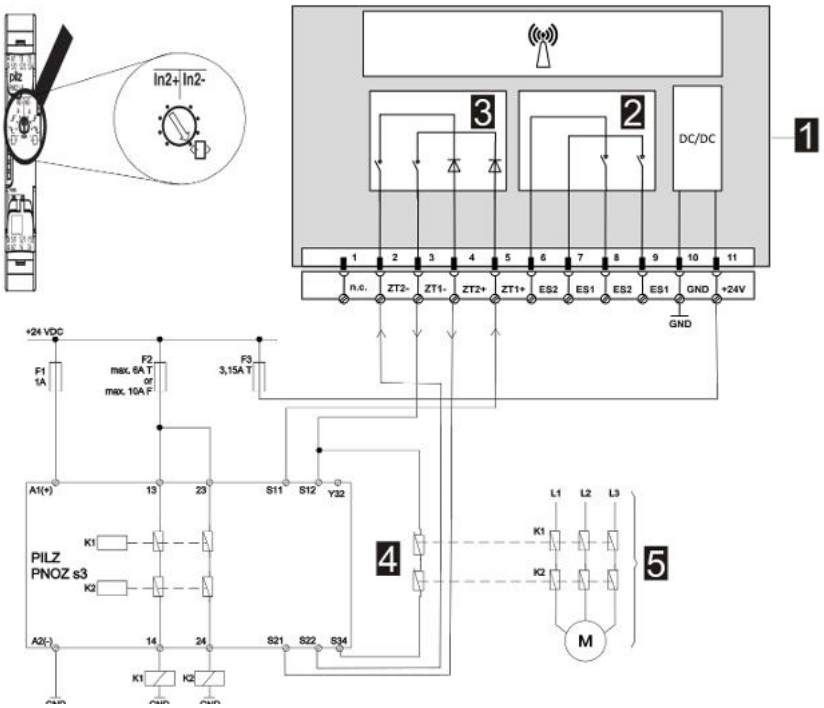


Fig. 5-38: Connection example for KeTop to PILZ PNOZ s3 monitoring device

1 ... Base station	2 ... Emergency stop
3 ... Enabling switch	4 ... Start condition with control monitoring
5 ... Enabling of the dangerous movement!	

KEBA © KEBA 2021

The graphic shows a circuit suggestion for achieving the Category 4 PL e for the enabling function with PILZ monitoring device. Also observe PILZ's operating instructions for the device PNOZ s3. For the calculation of the entire safety function "Enabling via enabling switch", the monitoring device and the following components are also to be taken into account.

Terminal assignment S1, see 5.8.1.1 Pin assignment.

5.8.11 Connection example for enabling function and emergency stop with KEBA safety control

When using the KEBA (D3-DU 3x5/x) safety control, the emergency stop can be connected to it in addition to the enabling switch.

The following example should serve as an aid for implementing this in the application.

© KEBA 2021

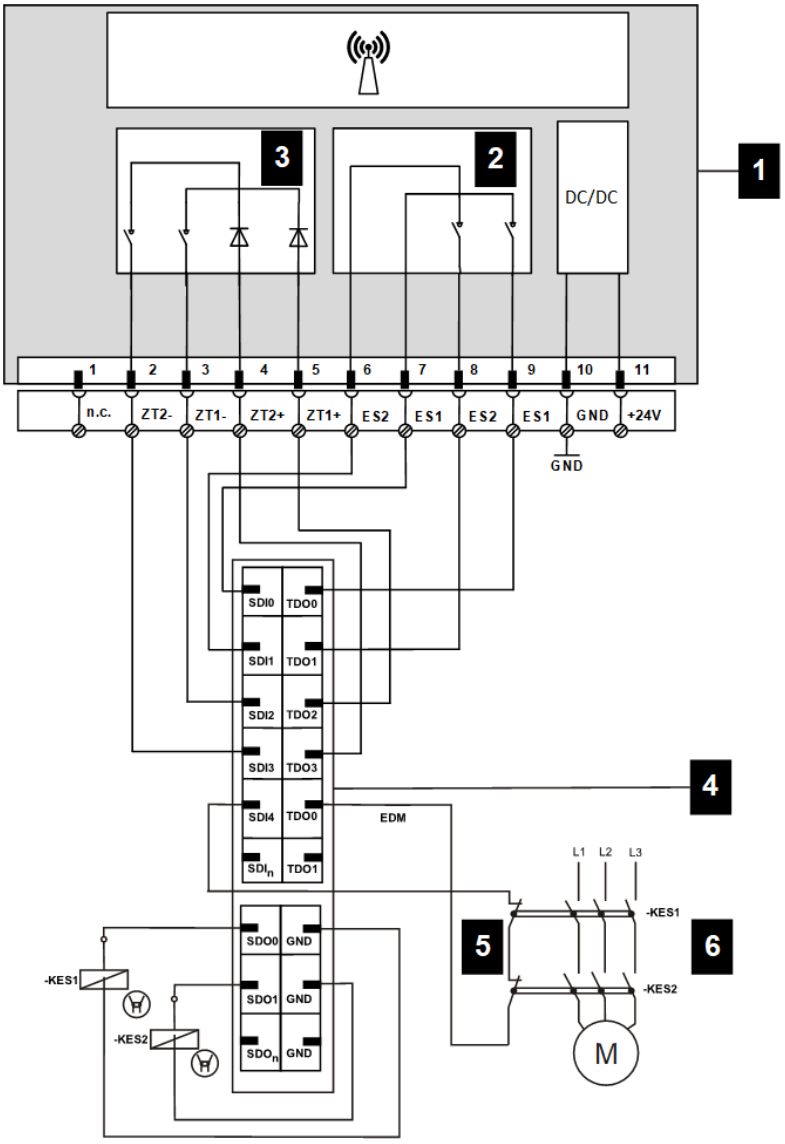


Fig. 5-39: Connection example with KEBA safety control (an enabling switch)

1 ... Base station	2 ... Emergency stop
3 ... Enabling switch	4 ... Safety control
5 ... EDM (External Device Monitoring)	6 ... Enabling of the dangerous movement!

The graphic shows a recommended switching setup for the enabling switch and the emergency stop using the safety control from KEBA.

KEBA © KEBA 2021

6 Base station CB42x

The CB42x is a base station that has an additional PROFINET / PROFIsafe gateway. The CB42x must only be used in the configuration with KEBA wireless handheld devices with an illuminated emergency stop.

The basestation is also available as variant CB421 with an additional cable outlet on the rear side.

The safety electronics of the emergency stop bypassing is designed with double circuits and facilitates implementation up to category 4 PL e in accordance with EN ISO 13849-1 or SIL 3 in accordance with EN 62061 / EN 61508.

6.1 Front view

Fig. 6-40: Front side

1 ... Status LEDs (PWR, SAFE, RNG)	2 ... Connection LEDs (ETH1, ETH2, WLAN)
3 ... Emergency stop	4 ... RFID sensor
5 ... Status LED bar	

© KEBA 2021

6.2 Rear view

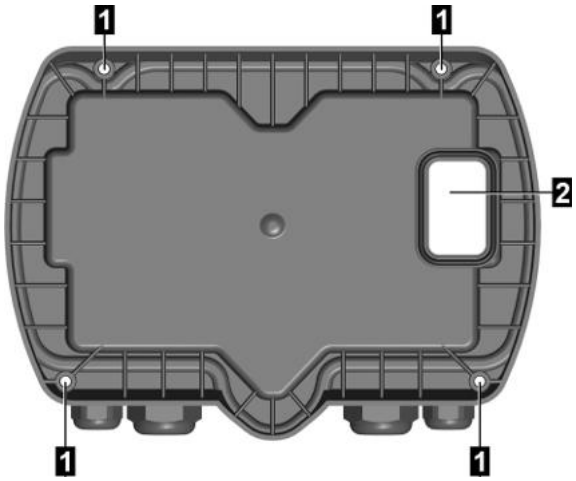


Fig. 6-41: Rear side

1 ... Drill holes	2 ... Cable outlet (only with CB421)

6.3 Bottom view

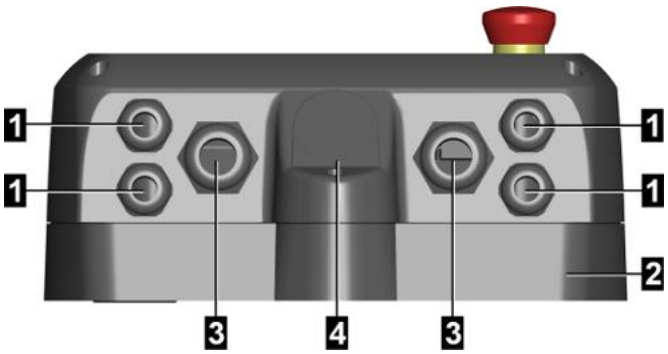


Fig. 6-42: Bottom

1 ... Standard cable outlets	2 ... PROFINET / PROFIsafe gateway
3 ... Ethernet cable outlets	4 ... "Pairing Reset" button (capacitive)

KEBA © KEBA 2021

6.4 Top view

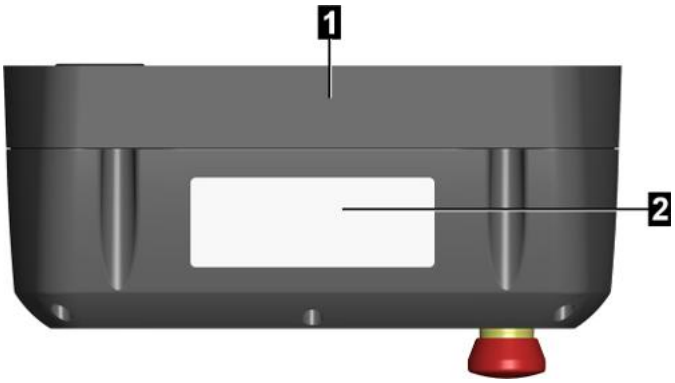


Fig. 6-43: Top

1 ... PROFINET / PROFIsafe gateway	2 ... Type plate

6.5 Type plate

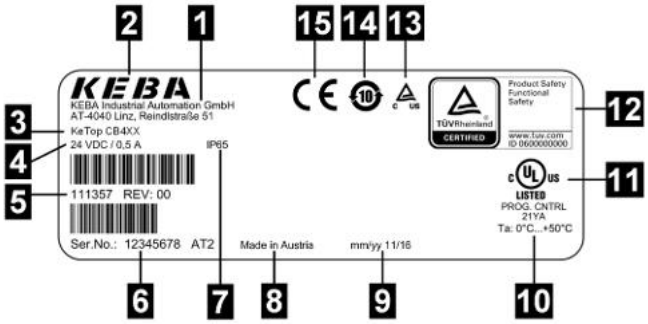


Fig. 6-44: Type plate

1 ... Manufacturer's address	2 ... Manufacturer
3 ... Product designation	4 ... Technical data (voltage / current)
5 ... Material and revision number	6 ... Serial number
7 ... Protection type	8 ... Country of manufacture
9 ... Production date	10 ... Ambient temperature
11 ... UL marking	12 ... TÜV marking
13 ... cTÜVus marking	14 ... China RoHS marking
15 ... CE marking of conformity	

6.6 Displays and operating elements

On the front side of the module, there are two LED groups and a status LED bar.

© KEBA 2021

6.6.1 Status LEDs

The base station is equipped with the following LEDs:

PWR (power supply)

LED	Description
Dark	No supply voltage, fault during startup
Green	Supply voltage present, device ready for operation

SAFE (secure connection)

LED	Description
Dark	No handheld device paired with the base station
Green	Handheld device continually paired
Green blinking	PROFINET SF/DCP

Information

A lighted SAFE LED indicates that the handheld terminal is safely connected ("paired") to a base station, even if there is no active wireless connection.

RNG (operation area monitoring)

LED	Description
Dark	No operation area monitoring configured or available
Green	Operation area monitoring active

6.6.2 Connection LEDs

ETH1 / ETH2

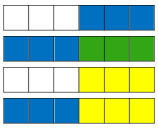
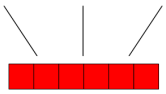
LED	Description
Dark	No Ethernet connection is available
Green	Active Ethernet connection (data transmission)

WLAN

LED	Description
Dark	WLAN module not available or not active
Green	WLAN module active

KEBA © KEBA 2021

6.6.3 Status LED bar

Bar display	Signal column	Meaning
Green	Green	"Normal" operating state (see 9.3 Base station operating states)
White	White	"Bridge active" operating state (see 9.3 Base station operating states)
Yellow LEDs going out successively	Yellow	"Pairing/Unpairing timer" operating state (see 9.3 Base station operating states)
Red	Red	"Estop" operating state (see 9.3 Base station operating states)
Yellow	Yellow	"Stop" mode No secure connection established with the safety control.
Flashing yellow	Yellow and white	"Standby" mode Fieldbus connection is established and safe state is signaled. No exchange of secure process data. User acknowledgment required.
	White and blue Blue and green White and yellow Blue and yellow	"Remote Pairing" special operating state These displays are optionally shown during a remote pairing process and are used for unique identification of the base station.
Blue	Blue	Error state (see 12 Diagnosis)
Half red / half blue	Red and blue	Error state (see 12 Diagnosis)
Flashing half yellow / half red	Yellow and Red	Error state (see 12 Diagnosis)
Flashing red 	Red and White	Error state (see 12 Diagnosis)
Red chaser light	Red	Error state (see 12 Diagnosis)

6.6.4 "Pairing Reset" button

The "Pairing Reset" button is used for manually forcing the handheld device to unpair. To do so, the "Pairing Reset" button must be held for > 5 s.

© KEBA 2021

This function is required if it is no longer possible for the handheld device to be unpaired from the base station on a regular basis (e.g. defect on the handheld device, handheld device physically too far away from base station, etc.). The function is available only if the base station no longer has any connection to the handheld device and is in the "Connection interrupted" state.

6.7 Mounting and installation instructions

WARNING!

The base station must not be installed in the hazard area of the machine.

6.7.1 Positioning the base station

The base station makes it possible for the handheld device to access the radio network. Correct positioning of the base station enables fault-free operation to the greatest extent possible.

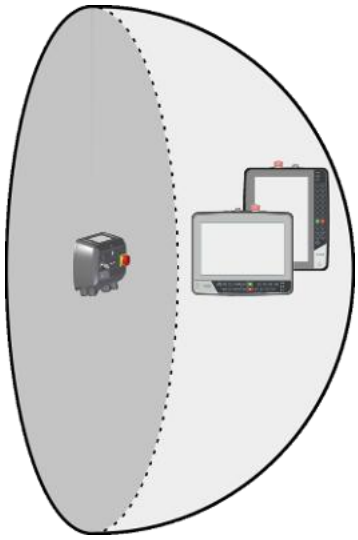


Fig. 6-45: Positioning the base station

The following points should be taken into account when selecting the position of the base station:

- The base station must be set up with a clear line of sight to the movement radius of the handheld device. The LED bar (or the signal column) must always be clearly visible from the hazard area.
- The base station should be installed as far away from large metal surfaces, glass surfaces or walls as possible.
- The base station must be installed in an unshielded area.
- The base stations themselves must be installed as far away from each other as possible. A minimum distance of 2 m must be maintained.

KEBA © KEBA 2021

- The distance to the nearest Wi-Fi connection (access point) must be at least 4 m.
- The minimum distance between the base station and objects or structural surroundings is 1 m above and below and 0.5 to the left and right.
- The base station should be easy to reach with the handheld device, since the pairing process must happen within a distance of 0 to 2 m between the base station and the handheld device.

6.7.2 Drilling template for wall mounting

The rear wall of the base station can be used to mark the drill holes.

The fastening material is dependent on the construction material of the mounting surface on which the base station is being installed.

We recommend mounting the rear wall using four M4 bolts with a maximum bolt head diameter of 9 mm. We recommend securing the bolts properly and with self-locking if the mounting surface is the wall of a control cabinet, for example.

6.7.3 Installing the base station

Remove housing

For the mounting and wiring of the base station, the housing must be removed from the rear wall. For this purpose, 6 PT30x10 screws must be removed from the front of the base station using a size 10 Torx key (see figure). The removed screws are required again for assembly.

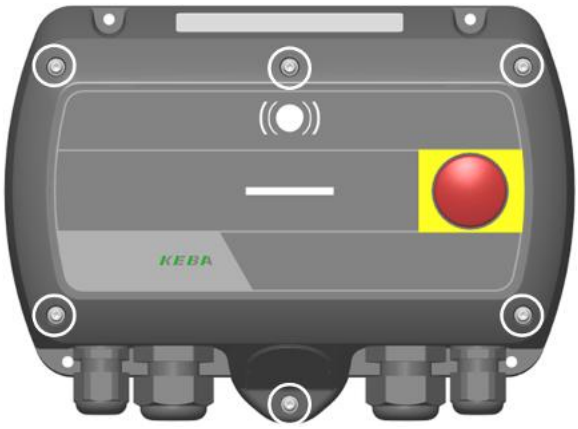


Fig. 6-46: Screws of the housing

Information

The base station is already wired between the housing and the rear wall. The connected cables can be disconnected during installation of the rear wall (see6.8.1 Internal wiring).

© KEBA 2021

Installing the rear wall

Information

A rear wall is available as an accessory for the base station, which enables rear wiring (see Rear wall for cable installation on rear).

The rear wall of the base station must be installed before the base station can be installed on the mounting surface. To do this, proceed as follows:

1) Mark the drill holes using the rear wall of the base station.
2) Drill the holes.
3) Insert the dowels into the holes, if necessary.
4) Install the rear wall on the wall using suitable screws, as shown in the following figure.

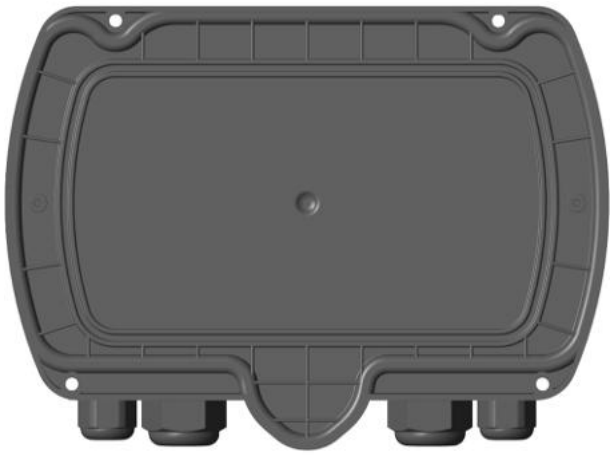


Fig. 6-47: Rear wall

The rear wall is now installed.

The wiring can then be executed, before the housing is closed (see Connections and wiring).

6.8 Connections and wiring

WARNING!

Faulty safety function!

Ensure that no pieces of wires, fillings or swarf fall into the device when you are drilling holes or connecting wires.

KEBA © KEBA 2021

ESD

Note the ESD notes in chapter 2.4 ESD information.

Caution

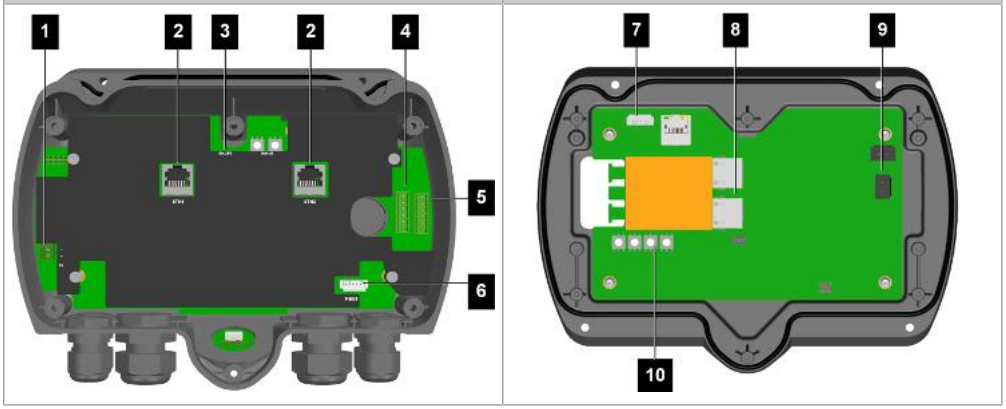
The wiring of the CB4xx can only be executed by qualified electricians in accordance with the information provided.

The following connections are available and can be guided individually to the outside using the cable outlets.

Information

Connection points, that are not numbered in the following illustration, must not be used.

CB42x base station connections with PROFINET / PROFIsafe gateway



1	Terminal strip S1 / power supply	2	Ethernet interface
3	DIP switch (operation area configuration)	4	Terminal strip S2
5	Terminal strip for "Signal" for external LED display	6	PROFINET / PROFIsafe gateway interface
7	CB42x interface	8	PROFINET interfaces
9	Power supply connection (VIN)	10	F-address switch

Wiring aid

The device can be turned over and attached to the installed rear wall for wiring.

For this purpose, the two upper holes on the front of the housing, used to bolt it in place, are attached to the two longer fastening pins on the rear wall.

© KEBA 2021

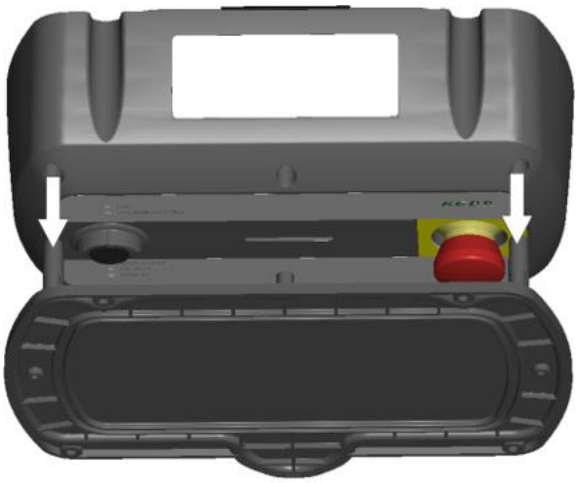


Fig. 6-48: Attaching to the rear wall

The cables are then fed through the corresponding cable outlets on the bottom of the device. These outlets have the following specifications:

Standard cable outlets

Clamping range (possible cable diameter):	4 to 8 mm
Degree of protection:	IP68
Size:	M16 x 1.5
Open-end wrench size:	SW19
Screw torque:	3 Nm

Ethernet cable outlets

Clamping range (possible cable diameter):	6 mm
Degree of protection:	IP68
Size:	M20 x 1.5
Max. diameter of RJ45 connector:	14.4 mm
Open-end wrench size:	SW27 (cap), SW24 (body)
Screw torque:	6 Nm

The screw connection must first be removed and pushed over the required cable so that the cables can be guided through the cable outlets. The seal ring, located in the cable outlet, must also be placed around Ethernet cables.

The cables can then be guided into the device, the screw connections can be tightened by hand again and the wiring can be implemented.

KEBA © KEBA 2021

Caution

Unused cable outlets must be sealed with the supplied blanking covers to ensure the protection class. To do this, remove the PG covers and install the blanking covers with the following torques (cross-slot size Z3):

- M16 × 1,5: 2 Nm
- M20 × 1,5: 2 Nm

6.8.1 Internal wiring

For the internal power supply and data transmission between CB42x and PROFINET / PROFIsafe gateway the following conntections are already connected:

Power supply

- Gateway connection: VIN plug - CB42x: terminal strip S1 (see 6.8.2.1 Pin assignment)

Data transmission

- Gateway connection: interface CB42x - CB42x: interface PROFINET / PROFIsafe gateway

6.8.2 Terminal strip S1 / power supply

For the CB42x, terminal strip S1 has 2 pins. The power is supplied through the VOUT plug on the PROFINET / PROFIsafe gateway and is routed from there to terminal S1.

WARNING!

Please observe the safety-relevant information in chapter 2.3 Personnel safety instructions.

If the base station is supplied with voltage, the PWR LED lights up green and the bar lights up white (= the emergency stop outputs of the base station are closed).

6.8.2.1 Pin assignment

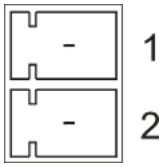


Fig. 6-49: Pin assignment

© KEBA 2021

Pin no.	Signal designation	Description
1	-	GND
2	+	24 V DC power supply

6.8.3 Terminal strip S2

Terminal strip S2 is directly wired and can be used for safety functions.

If the base station is equipped with an optional key-operated switch, the operating element signals are provided at terminal S2. The position of the key-operated switch is specified by combining the levels of two contacts (see 6.8.3.1 Pin assignment).

6.8.3.1 Pin assignment

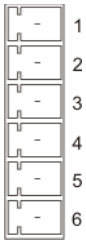
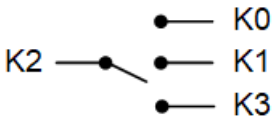


Fig. 6-50: Pin assignment

Pin No.	Signal designation	Description
1	GND	Grounding
2	n.a.	No use possible
3	K3	Key-operated switch contact: Position 3 (right switch position) 
4	K2	Key-operated switch contact: COMMON
5	K1	Key-operated switch contact: Position 2 (middle switch position)
6	K0	Key-operated switch contact: Position 1 (left switch position)

6.8.4 "Signal" terminal strip

At the "Signal" terminal, a signal column can be connected.

The base station has been tested by KEBA with the following signal columns:

KEBA © KEBA 2021

Manufacturer	Product designation
PATLITE	LR4-_02LJN
SPÄLTI	MES-502A-RYGBC(DC24V)

The use of these signal columns is recommended. Refer to the documentation from the manufacturer for more information.

Information

The "Signal" terminal strip may only be used to connect a signal column for displaying the operating and diagnostic states of the base station.

6.8.4.1 Pin assignment

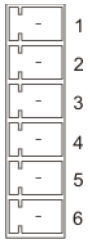


Fig. 6-51: Pin assignment

Pin No.	Signal designation	Description
1	24 V	24 V DC power supply
2	WH	Signal color: transparent/white
3	BU	Signal color: blue
4	Y/O	Signal color: yellow
5	GN	Signal color: green
6	RD	Signal color: red

6.8.5 Ethernet

The device provides 2 Ethernet interfaces. They are provided to connect devices with which the handheld device should communicate. The interfaces can be fed through the cable outlets to the outside.

6.8.5.1 Pin assignment

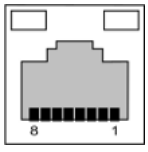


Fig. 6-52: RJ45 plug socket

© KEBA 2021

Pin no.	Signal designation		Input / Output
1	Tr. Data+	Transmit Data +	Output
2	Tr. Data-	Transmit Data -	Output
3	Re. Data+	Receive Data +	Input
4	n.c.	n.c.	---
5	n.c.	n.c.	---
6	Re. Data-	Receive Data -	Input
7	n.c.	n.c.	---
8	n.c.	n.c.	---

6.8.6 PROFINET

The gateway module has 2 PROFINET interfaces. The interfaces can be routed to the outside via the cable outlets on the CB42x or through the outlet (optional) on the back of the PROFINET / PROFIsafe gateway.

The following connectors can be used:

Manufacturer	Product designation
Siemens	6GK1901-1BB10-2AA0 (FastConnect)
Weidmüller	IE-PS-RJ45-FH-BK

Caution

Cable ties must be used on the tabs on the print to relieve the strain on the connected cables.

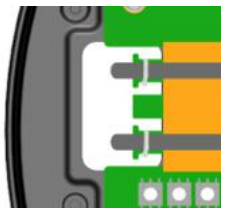


Fig. 6-53: Example: Example: Two connected cables with cable ties as strain relief

KEBA © KEBA 2021

6.8.7 Changes to the wiring

Information

Information about changes to the wiring:

- When disconnecting plug connections, be sure to use your fingers to unplug the connector from its wires (do not use sharp objects to help with this process).
- When disconnecting the RJ45 connectors, it must be ensured that the locking lever is activated during the process.

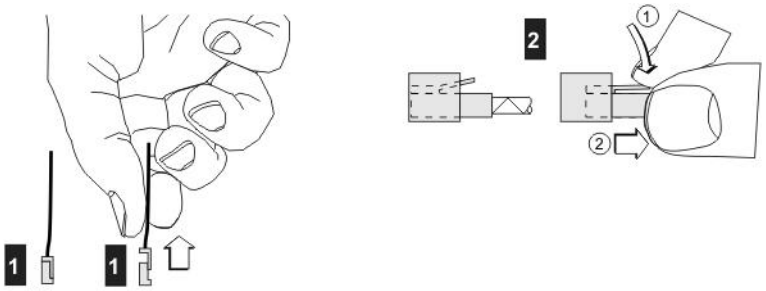


Fig. 6-54: Disconnecting the main plug and RJ-45 connector

1 ... Main plug	2 ... RJ45 connectors

6.8.8 Closing the base station

The housing must be removed from the rear wall and turned over to close the base station. The housing can then be placed on the rear wall and secured using 6 PT30x10 screws (required tool - Torx size 10) as shown in the diagram. The screws are included in the scope of delivery.

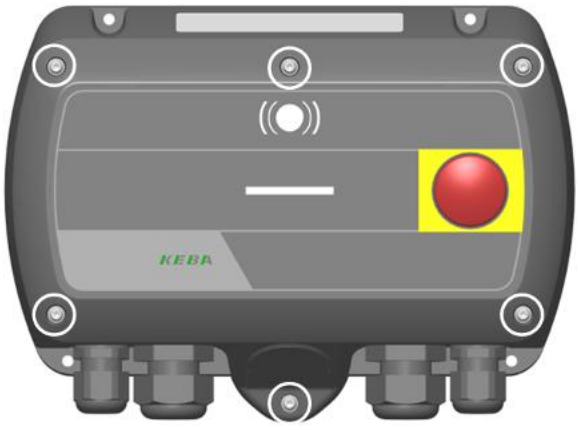


Fig. 6-55: Screws for closing

© KEBA 2021

Information

Information on closing the base station:

- The seal must be clean, undamaged and in the correct position.
- No cables must be trapped.
- The base station must be screwed together again using all PT30x10 screws (torque: 0.85 Nm - 1.15 Nm). This is the only way to ensure the corresponding protection class.

The base station is ready for operation.

6.8.9 Emergency stop

The base station is equipped with an emergency stop.

WARNING!

Non-functional emergency stop systems can have fatal consequences! The red-yellow designated emergency stop must be operative at all times and in all operating modes of a machine or system.

WARNING!

The emergency stop on the non-connected handheld device does not replace the emergency stop on the machine. A fixed, hardwired emergency stop must always be available on the machine.

6.9 Error acknowledgement

WARNING!

Risk of death due to unexpected start of the machine

If the CB4xx is re-integrated, for example after a bus error, the CB4xx is set to the previous state. Without a higher level saftey measure, the machine can unexpectedly start and lead to injuries or death.

- Make sure that the used safety control does not automatically re-integrate the F device.

Every error that occurs locally in the wireless system, must be acknowledged at the CB4xx or at the handheld device. These errors are displayed at the CB4xx as a red/yellow LED bar.

KEBA © KEBA 2021

The acknowledgement is performed by pressing/unlocking the emergency stop-button. A successfull acknowledgement is displayed at the CB4xx by a yellow blinking LED bar. Only after this acknowledgement, software acknowledgement at the F host is possible by setting a user acknowledgement.

© KEBA 2021

7 Base station CB43x

The CB43x is a base station that has an additional EtherCAT/FSoE gateway. The CB43x must only be used in the configuration with KEBA wireless handheld devices with an illuminated emergency stop.

The basestation is also available as variant CB431 with an additional cable outlet on the rear side.

As a safety measure, the base station is equipped with an emergency stop. The safety electronics of the emergency stop bypassing is designed with double circuits and facilitates implementation up to category 4 PL e in accordance with EN ISO 13849-1 or SIL 3 in accordance with EN 62061 / EN 61508.

7.1 Front view

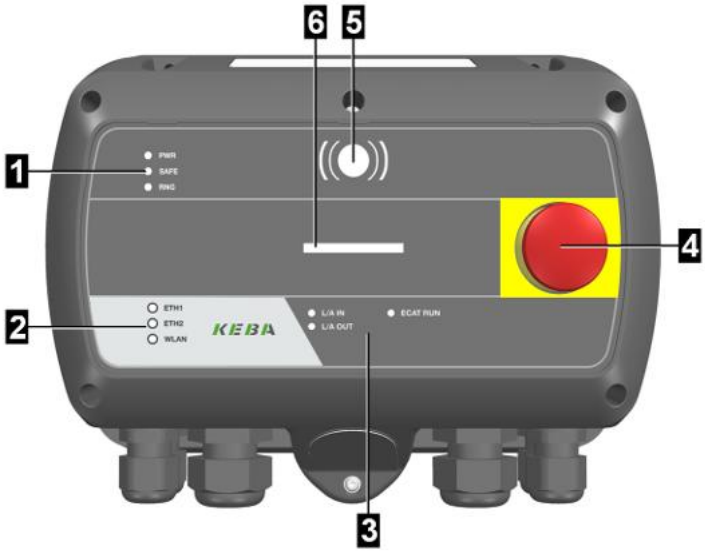


Fig. 7-56: Front view

1 ... Status LEDs (PWR, SAFE, RNG)	2 ... Connection LEDs (ETH1, ETH2, WLAN)
3 ... EtherCAT LEDs	4 ... Emergency stop
5 ... RFID sensor	6 ... Status LED bar

KEBA © KEBA 2021

7.2 Rear view

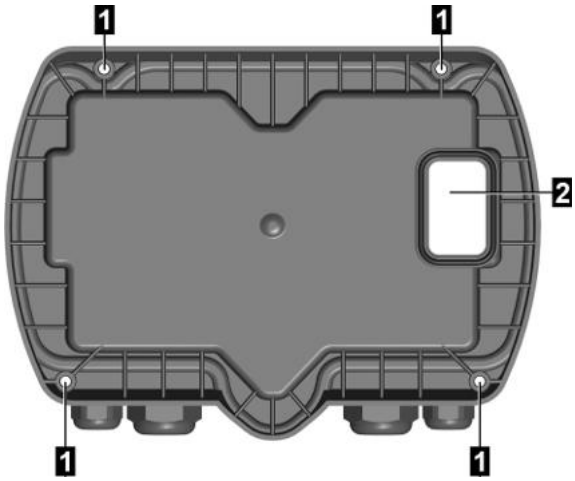


Fig. 7-57: Rear side

1 ... Drill holes	2 ... Cable outlet (only with CB431)

7.3 Bottom view

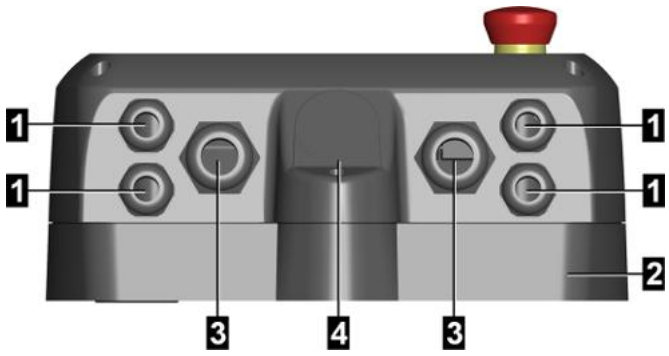


Fig. 7-58: Bottom

1 ... Standard cable outlets	2 ... EtherCAT / FSoE gateway
3 ... Ethernet cable outlets	4 ... "Pairing Reset" button (capacitive)

© KEBA 2021

7.4 Top view

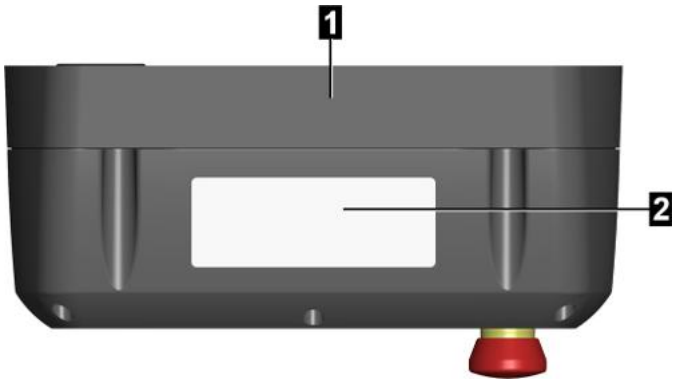


Fig. 7-59: Top

1 ... EtherCAT / FSoE gateway	2 ... Type plate

7.5 Type plate

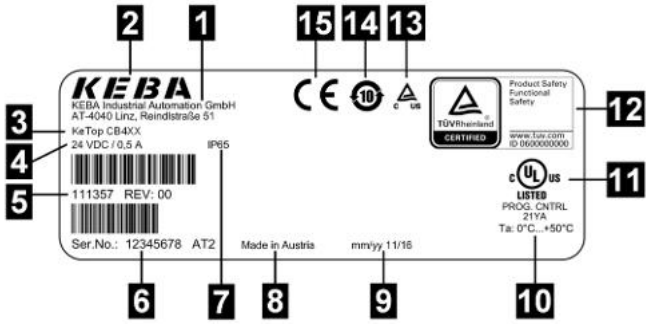


Fig. 7-60: Type plate

1 ... Manufacturer's address	2 ... Manufacturer
3 ... Product designation	4 ... Technical data (voltage / current)
5 ... Material and revision number	6 ... Serial number
7 ... Protection type	8 ... Country of manufacture
9 ... Production date	10 ... Ambient temperature
11 ... UL marking	12 ... TÜV marking
13 ... cTÜVus marking	14 ... China RoHS marking
15 ... CE marking of conformity	

7.6 Displays and operating elements

On the front side of the module, there are two LED groups and a status LED bar.

KEBA © KEBA 2021

7.6.1 Status LEDs

The base station is equipped with the following LEDs:

PWR (power supply)

LED	Description
Dark	No supply voltage, fault during startup
Green	Supply voltage present, device ready for operation

SAFE (secure connection)

LED	Description
Dark	No handheld device paired with the base station
Green	Handheld device continually paired

Information

A lighted SAFE LED indicates that the handheld terminal is safely connected ("paired") to a base station, even if there is no active wireless connection.

RNG (operation area monitoring)

LED	Description
Dark	No operation area monitoring configured or available
Green	Operation area monitoring active

7.6.2 Connection LEDs

ETH1 / ETH2

LED	Description
Dark	No Ethernet connection is available
Green	Active Ethernet connection (data transmission)

WLAN

LED	Description
Dark	WLAN module not available or not active
Green	WLAN module active

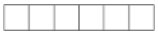
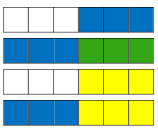
EtherCAT

LED	Description
L/A IN	
• Dark	No link established

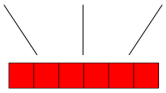
© KEBA 2021

LED	Description
• Green blinking	Device receives ethernet frames
• Green	Link established
L/A OUT	
• Dark	No link established
• Green blinking	Device sends ethernet frames
• Green	Link established
ECAT RUN	
• Dark	Operating state "INIT"
• Green blinking	Operating state "PRE-OPERATIONAL"
• Green flash blinking (200 ms on, 1000 ms off)	Operating state "SAFE-OPERATIONAL"
• Green	Operating state "OPERATIONAL"

7.6.3 Status LED bar

Bar display	Signal column	Meaning
Green	Green	"Normal" operating state (see 9.3 Base station operating states)
White 	White	"Bridge active" operating state (see 9.3 Base station operating states)
Yellow LEDs going out successively	Yellow	"Pairing/Unpairing timer" operating state (see 9.3 Base station operating states)
Red	Red	"Estop" operating state (see 9.3 Base station operating states)
Yellow	Yellow	"Stop" mode No secure connection established with the safety control.
Flashing yellow	Yellow and white	"Standby" mode Fieldbus connection is established and safe state is signaled. No exchange of secure process data. User acknowledgment required.
	White and blue Blue and green White and yellow Blue and yellow	"Remote Pairing" special operating state These displays are optionally shown during a remote pairing process and are used for unique identification of the base station.
Blue	Blue	Error state (see 12 Diagnosis)
Half red / half blue	Red and blue	Error state (see 12 Diagnosis)

KEBA © KEBA 2021

Bar display	Signal column	Meaning
Flashing half yellow / half red	Yellow and Red	Error state (see 12 Diagnosis)
Flashing red 	Red and White	Error state (see 12 Diagnosis)
Red chaser light	Red	Error state (see 12 Diagnosis)

7.6.4 "Pairing Reset" button

The "Pairing Reset" button is used for manually forcing the handheld device to unpair. To do so, the "Pairing Reset" button must be held for > 5 s.

This function is required if it is no longer possible for the handheld device to be unpaired from the base station on a regular basis (e.g. defect on the handheld device, handheld device physically too far away from base station, etc.). The function is available only if the base station no longer has any connection to the handheld device and is in the "Connection interrupted" state.

7.7 Mounting and installation instructions

WARNING!

The base station must not be installed in the hazard area of the machine.

7.7.1 Positioning the base station

The base station makes it possible for the handheld device to access the radio network. Correct positioning of the base station enables fault-free operation to the greatest extent possible.

© KEBA 2021

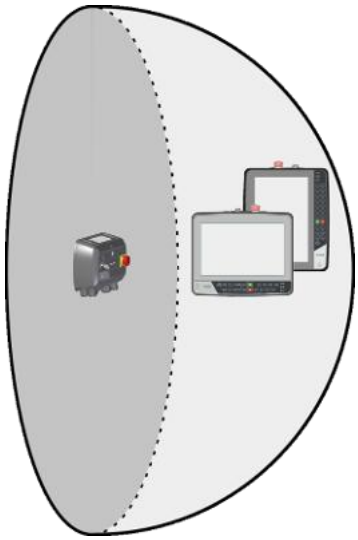


Fig. 7-61: Positioning the base station

The following points should be taken into account when selecting the position of the base station:

- The base station must be set up with a clear line of sight to the movement radius of the handheld device. The LED bar (or the signal column) must always be clearly visible from the hazard area.
- The base station should be installed as far away from large metal surfaces, glass surfaces or walls as possible.
- The base station must be installed in an unshielded area.
- The base stations themselves must be installed as far away from each other as possible. A minimum distance of 2 m must be maintained.
- The distance to the nearest Wi-Fi connection (access point) must be at least 4 m.
- The minimum distance between the base station and objects or structural surroundings is 1 m above and below and 0.5 to the left and right.
- The base station should be easy to reach with the handheld device, since the pairing process must happen within a distance of 0 to 2 m between the base station and the handheld device.

7.7.2 Drilling template for wall mounting

The rear wall of the base station can be used to mark the drill holes.

The fastening material is dependent on the construction material of the mounting surface on which the base station is being installed.

We recommend mounting the rear wall using four M4 bolts with a maximum bolt head diameter of 9 mm. We recommend securing the bolts properly and with self-locking if the mounting surface is the wall of a control cabinet, for example.

KEBA © KEBA 2021

7.7.3 Installing the base station

Remove housing

For the mounting and wiring of the base station, the housing must be removed from the rear wall. For this purpose, 6 PT30x10 screws must be removed from the front of the base station using a size 10 Torx key (see figure). The removed screws are required again for assembly.

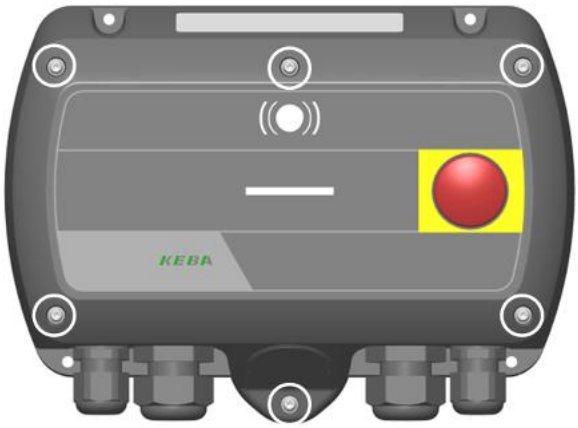


Fig. 7-62: Screws of the housing

Information

The base station is already wired between the housing and the rear wall. The connected cables can be disconnected during installation of the rear wall (see6.8.1 Internal wiring).

Installing the rear wall

Information

A rear wall is available as an accessory for the base station, which enables rear wiring (see Rear wall for cable installation on rear).

The rear wall of the base station must be installed before the base station can be installed on the mounting surface. To do this, proceed as follows:

1) Mark the drill holes using the rear wall of the base station.
2) Drill the holes.
3) Insert the dowels into the holes, if necessary.
4) Install the rear wall on the wall using suitable screws, as shown in the following figure.

© KEBA 2021

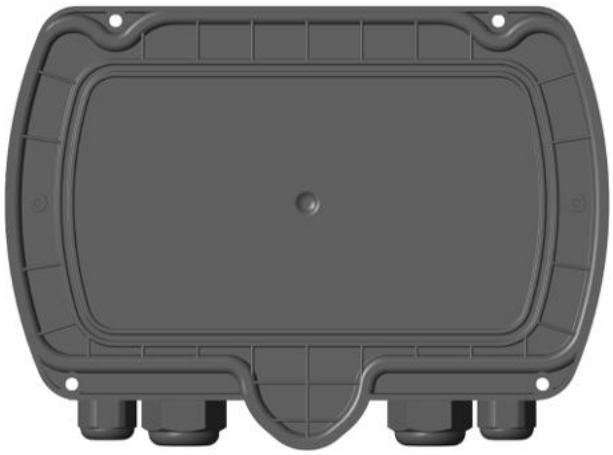


Fig. 7-63: Rear wall

The rear wall is now installed.

The wiring can then be executed, before the housing is closed (see Connections and wiring).

7.8 Connections and wiring

WARNING!

Faulty safety function!

Ensure that no pieces of wires, fillings or swarf fall into the device when you are drilling holes or connecting wires.

ESD

Note the ESD notes in chapter 2.4 ESD information.

Caution

The wiring of the CB4xx can only be executed by qualified electricians in accordance with the information provided.

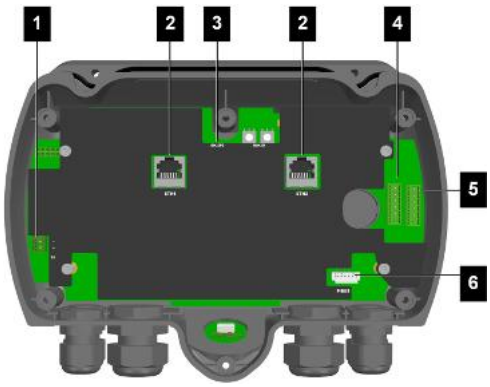
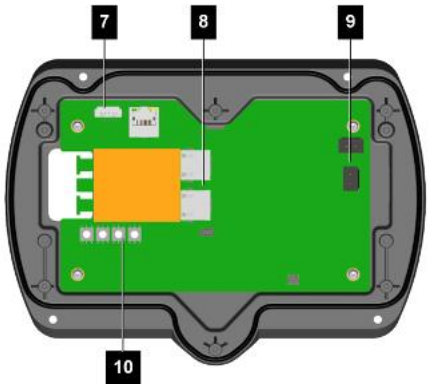
The following connections are available and can be guided individually to the outside using the cable outlets.

Information

Connection points, that are not numbered in the following illustration, must not be used.

KEBA © KEBA 2021

CB43x base station connections with EtherCAT / FSoE gateway

CB43x	EtherCAT / FSoE gateway
	

1	Terminal strip S1 / power supply	2	Ethernet interface
3	DIP switch (operation area configuration)	4	Terminal strip S2
5	Terminal strip for "Signal" for external LED display	6	EtherCAT / FSoE gateway interface
7	CB43x interface	8	EtherCAT interfaces
9	Power supply connection (VIN)	10	F-address switch

One of the two EtherCAT interfaces is used to connect an EtherCAT or FSoE master. The second interface can be used to connect additional EtherCAT devices using parallel or tree topology.

Wiring aid

The device can be turned over and attached to the installed rear wall for wiring.

For this purpose, the two upper holes on the front of the housing, used to bolt it in place, are attached to the two longer fastening pins on the rear wall.

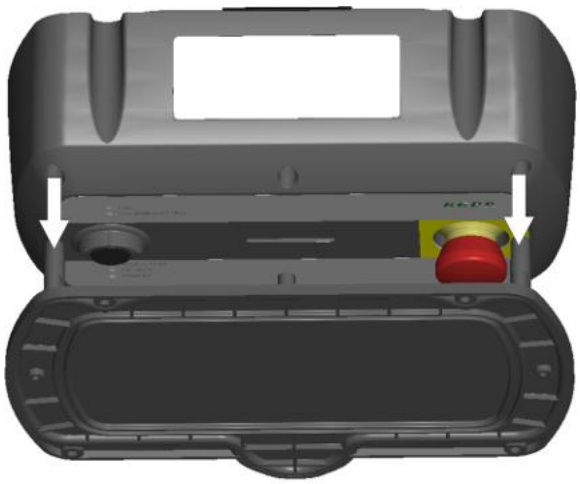


Fig. 7-64: Attaching to the rear wall

© KEBA 2021

The cables are then fed through the corresponding cable outlets on the bottom of the device. These outlets have the following specifications:

Standard cable outlets

Clamping range (possible cable diameter):	4 to 8 mm
Degree of protection:	IP68
Size:	M16 x 1.5
Open-end wrench size:	SW19
Screw torque:	3 Nm

Ethernet cable outlets

Clamping range (possible cable diameter):	6 mm
Degree of protection:	IP68
Size:	M20 x 1.5
Max. diameter of RJ45 connector:	14.4 mm
Open-end wrench size:	SW27 (cap), SW24 (body)
Screw torque:	6 Nm

The screw connection must first be removed and pushed over the required cable so that the cables can be guided through the cable outlets. The seal ring, located in the cable outlet, must also be placed around Ethernet cables.

The cables can then be guided into the device, the screw connections can be tightened by hand again and the wiring can be implemented.

Caution

Unused cable outlets must be sealed with the supplied blanking covers to ensure the protection class. To do this, remove the PG covers and install the blanking covers with the following torques (cross-slot size Z3):

- M16 × 1,5: 2 Nm
- M20 × 1,5: 2 Nm

7.8.1 Internal wiring

For the internal power supply and data transmission between CB43x and EtherCAT / FSoE gateway the following conntections are already connected:

Power supply

- Gateway connection: VIN plug - CB43x: terminal strip S1 (see 7.8.2.1 Pin assignment)

Data transmission

- Gateway connection: interface CB43x - CB43x: interface EtherCAT / FSoE gateway

KEBA © KEBA 2021

7.8.2 Terminal strip S1 / power supply

For the CB43x, terminal strip S1 has 2 pins. The power is supplied through the VOUT plug on the EtherCAT / FSoE gateway and is routed from there to terminal S1.

WARNING!

Please observe the safety-relevant information in chapter 2.3 Personnel safety instructions.

If the base station is supplied with voltage, the PWR LED lights up green and the bar lights up white (= the emergency stop outputs of the base station are closed).

7.8.2.1 Pin assignment

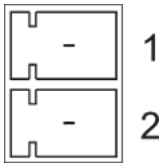


Fig. 7-65: Pin assignment

Pin no.	Signal designation	Description
1	-	GND
2	+	24 V DC power supply

7.8.3 Terminal strip S2

Terminal strip S2 is directly wired and can be used for safety functions.

If the base station is equipped with an optional key-operated switch, the operating element signals are provided at terminal S2. The position of the key-operated switch is specified by combining the levels of two contacts (see 7.8.3.1 Pin assignment).

7.8.3.1 Pin assignment

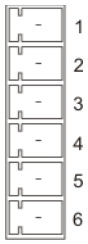
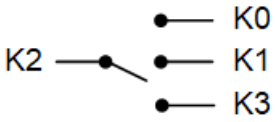


Fig. 7-66: Pin assignment

© KEBA 2021

Pin No.	Signal designation	Description
1	GND	Grounding
2	n.a.	No use possible
3	K3	Key-operated switch contact: Position 3 (right switch position) 
4	K2	Key-operated switch contact: COMMON
5	K1	Key-operated switch contact: Position 2 (middle switch position)
6	K0	Key-operated switch contact: Position 1 (left switch position)

7.8.4 "Signal" terminal strip

At the "Signal" terminal, a signal column can be connected.

The base station has been tested by KEBA with the following signal columns:

Manufacturer	Product designation
PATLITE	LR4-_02LJN
SPÄLTI	MES-502A-RYGBC(DC24V)

The use of these signal columns is recommended. Refer to the documentation from the manufacturer for more information.

Information

The "Signal" terminal strip may only be used to connect a signal column for displaying the operating and diagnostic states of the base station.

7.8.4.1 Pin assignment

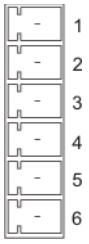


Fig. 7-67: Pin assignment

KEBA © KEBA 2021

Pin No.	Signal designation	Description
1	24 V	24 V DC power supply
2	WH	Signal color: transparent/white
3	BU	Signal color: blue
4	Y/O	Signal color: yellow
5	GN	Signal color: green
6	RD	Signal color: red

7.8.5 Ethernet

The device provides 2 Ethernet interfaces. They are provided to connect devices with which the handheld device should communicate. The interfaces can be fed through the cable outlets to the outside.

7.8.5.1 Pin assignment

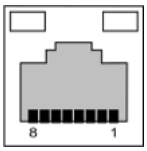


Fig. 7-68: RJ45 plug socket

Pin no.	Signal designation		Input / Output
1	Tr. Data+	Transmit Data +	Output
2	Tr. Data-	Transmit Data -	Output
3	Re. Data+	Receive Data +	Input
4	n.c.	n.c.	---
5	n.c.	n.c.	---
6	Re. Data-	Receive Data -	Input
7	n.c.	n.c.	---
8	n.c.	n.c.	---

7.8.6 EtherCAT

The gateway module has 2 EtherCAT interfaces. The interfaces can be routed to the outside via the cable outlets on the CB43x or through the outlet (optional) on the back of the EtherCAT gateway.

The following connectors can be used:

Manufacturer	Product designation
Siemens	6GK1901-1BB10-2AA0 (FastConnect)
Weidmüller	IE-PS-RJ45-FH-BK

© KEBA 2021

Caution

Cable ties must be used on the tabs on the print to relieve the strain on the connected cables.

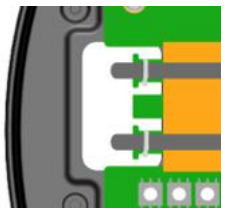


Fig. 7-69: Example: Example: Two connected cables with cable ties as strain relief

7.8.7 Changes to the wiring

Information

Information about changes to the wiring:

- When disconnecting plug connections, be sure to use your fingers to unplug the connector from its wires (do not use sharp objects to help with this process).
- When disconnecting the RJ45 connectors, it must be ensured that the locking lever is activated during the process.

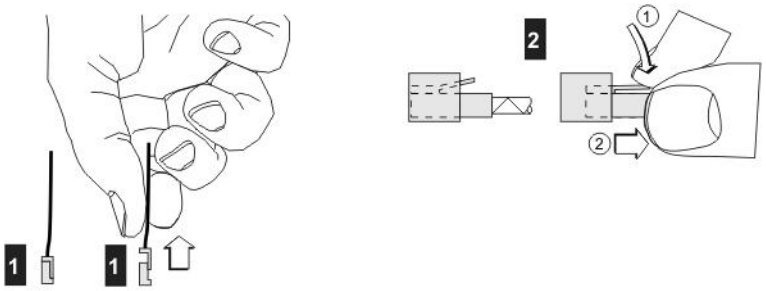


Fig. 7-70: Disconnecting the main plug and RJ-45 connector

1 ... Main plug	2 ... RJ45 connectors

7.8.8 Closing the base station

The housing must be removed from the rear wall and turned over to close the base station. The housing can then be placed on the rear wall and secured using 6 PT30x10 screws (required tool - Torx size 10) as shown in the diagram. The screws are included in the scope of delivery.

KEBA © KEBA 2021

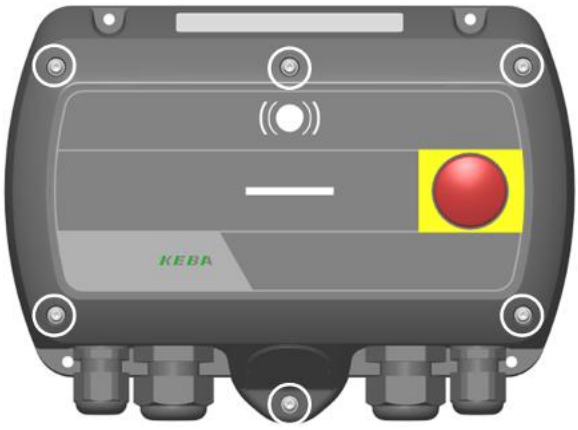


Fig. 7-71: Screws for closing

Information

Information on closing the base station:

- The seal must be clean, undamaged and in the correct position.
- No cables must be trapped.
- The base station must be screwed together again using all PT30x10 screws (torque: 0.85 Nm - 1.15 Nm). This is the only way to ensure the corresponding protection class.

The base station is ready for operation.

7.8.9 Emergency stop

The base station is equipped with an emergency stop.

WARNING!

Non-functional emergency stop systems can have fatal consequences! The red-yellow designated emergency stop must be operative at all times and in all operating modes of a machine or system.

WARNING!

The emergency stop on the non-connected handheld device does not replace the emergency stop on the machine. A fixed, hardwired emergency stop must always be available on the machine.

© KEBA 2021

7.9 Error acknowledgement

WARNING!

Risk of death due to unexpected start of the machine

If the CB4xx is re-integrated, for example after a bus error, the CB4xx is set to the previous state. Without a higher level saftey measure, the machine can unexpectedly start and lead to injuries or death.

- Make sure that the used safety control does not automatically re-integrate the F device.

Every error that occurs locally in the wireless system, must be acknowledged at the CB4xx or at the handheld device. These errors are displayed at the CB4xx as a red/yellow LED bar.

The acknowledgement is performed by pressing/unlocking the emergency stop-button. A successfull acknowledgement is displayed at the CB4xx by a yellow blinking LED bar. Only after this acknowledgement, software acknowledgement at the F host is possible by setting a user acknowledgement.

KEBA © KEBA 2021

8 Configuration

8.1 Box ID configuration

The base station features 2 address switches for configuring the box ID.

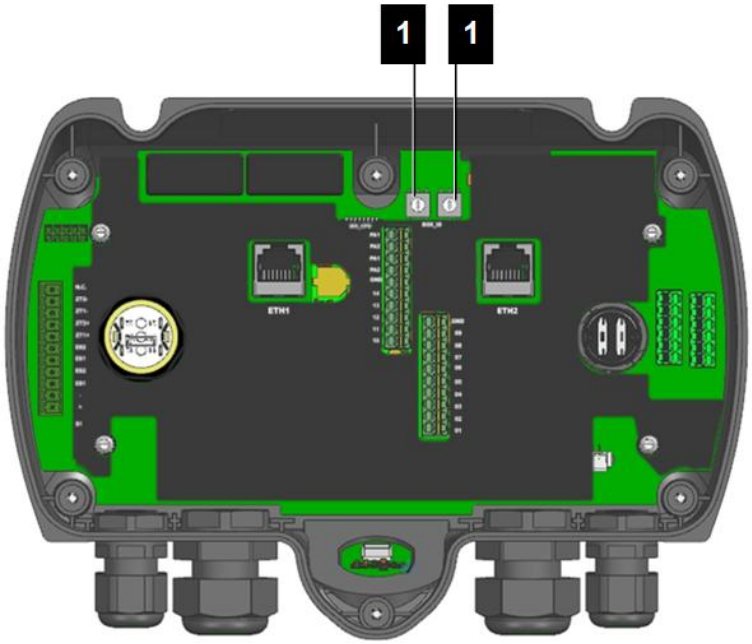


Fig. 8-72: Position of the configuration elements

1 ... Address switch	

The configuration of the box ID is used to identify the device. An ID of 0 to 255 can be assigned and used in the application. Two address switches are provided to set the address as a hexadecimal value.

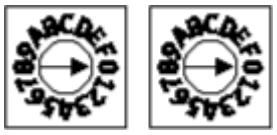


Fig. 8-73: Address switch

The box ID 00 is set as standard.

Examples:

Left address switch	Right address switch	Address
0	0	0
0	1	1
0	2	2

© KEBA 2021

Left address switch	Right address switch	Address
...	...	...
0	A	10
...	...	...
1	0	16
1	1	17
...	...	..

When establishing a connection with the handheld device (pairing / remote pairing), the current box ID is transmitted.

An evaluation can be done using the connection protocols or the "HWApi" interface.

8.2 F addressing (only for CB42x and CB43x)

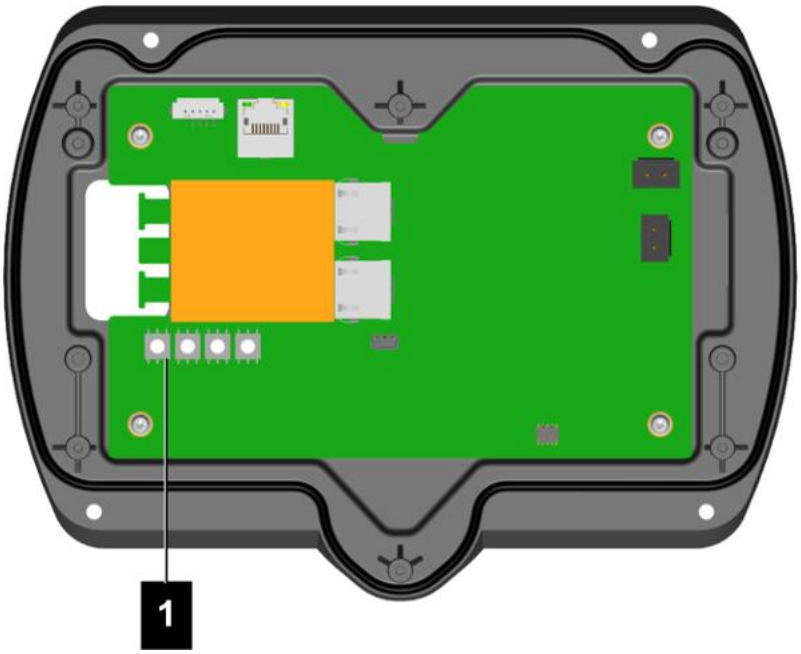
The gateway module has 4 address switches for setting the F addresses of the respective bus participants. The F addresses are set in hexadecimal.

In the delivery state the F addressing is 0 by default.

Information

The F-address 0000 is not permitted. An invalid F-address can lead to a fieldbus error and is indicated via the status LED bar of the base station.

KEBA © KEBA 2021



1 ... Adress switch	

To change the F address of a bus device, proceed as follows:

1) Set all address switches to "0". (Delivery state: all address switches are set to 0)
2) Restart base station and wait 10 seconds.
3) De-energize the base station.
4) Enter the desired F address via the address switches.

The next time the base station is switched on, the LED status bar flashes red. After a restart, the new F address is valid.

For an example about address assignment with address switches, see 8.1 Box ID configuration.

8.3 Operation area configuration (safety-related)

The DIP switch on the base station can be used to configure the operation area of the base station with the handheld device. The operation area must be configured during the process of commissioning the base station. If no operation area is defined, the status LED bar on the base station flashes white.

Operation area	Bit 0	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7
Without	ON	OFF	OFF	OFF	x	x	x	x
Initial state (safe state)	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

Operation area	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 of the respective switch is irrelevant

ON/OFF position of the switches

The following illustration shows the position of the DIP switch in the open base station and the configuration of the operating zone.

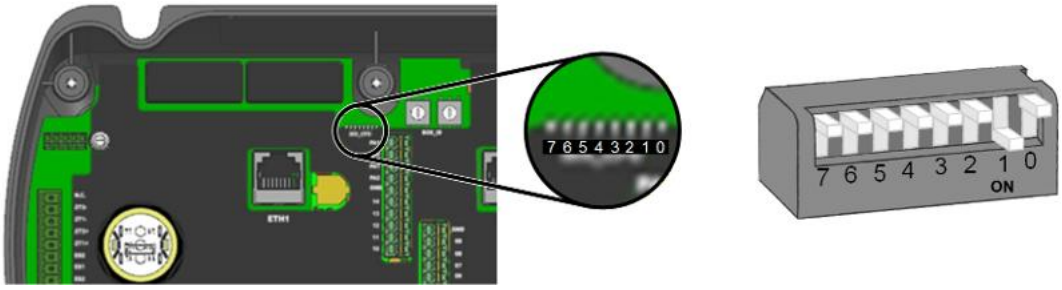


Fig. 8-74: Example: Position of the DIP switch and operation area configured as 5 m

To configure the operation area, you must de-energize the base station. Proceed as follows:

1) Set all DIP switches to OFF
2) Supply the base station with voltage and wait approx. 10 seconds
3) De-energize the base station
4) Set DIP switches to the desired operation area

The next time the base station is switched on, the configuration is applied.

8.4 Device configuration (Device Config)

In the device configuration on the handheld device, the following basic configurations can be carried out:

- Base station settings
- Generate diagnostic data
- Adjusting the display brightness of the handheld device
- Display of license information
- Network settings
- Triggering a restart of the handheld device
- Shutting down the handheld device
- Display of the software versions

KEBA © KEBA 2021

Information

To ensure the ability to use all configuration options, the handheld device must be paired with the base station before device configuration is begun.

The device configuration can be started from the desktop by double-clicking the **DeviceConfig** icon.

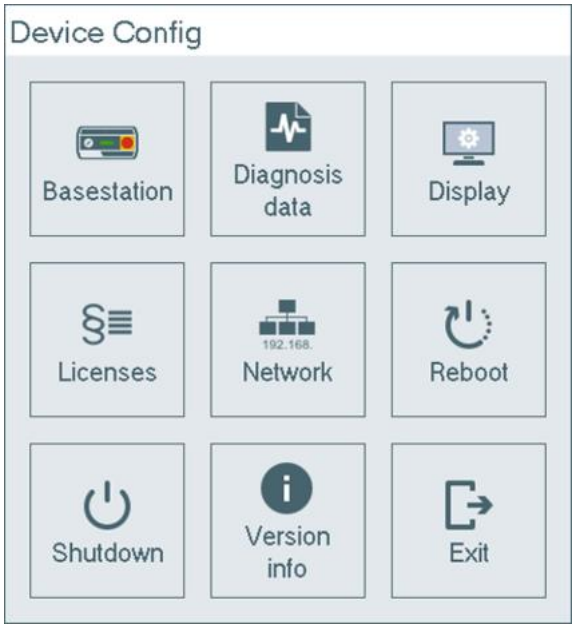


Fig. 8-75: Device configuration main menu

Use **Exit** to leave the device configuration.

8.4.1 Base station

Pressing **Base station** calls up the base station window. In this window, configurations can be carried out for the base station.

Information

To do so, the handheld device must be paired with the base station.

© KEBA 2021

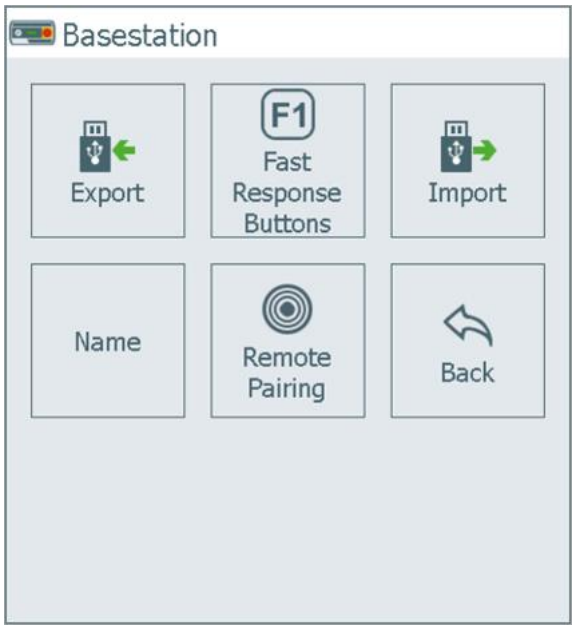


Fig. 8-76: Base station window

Designation	Meaning
Export	Exports the settings of the paired base station to a file. You can select which information is to be stored in the file. Only one mass storage device at the USB hub (e.g. USB stick) may be used as the storage location. If no base station is paired, this function cannot be selected.
Fast response buttons	Configuration of the buttons that are output directly to outputs of the base station (optional).
Import	Imports the settings for the paired base station from a file. You can select which information stored in the file is to be imported. Only one mass storage device at the USB hub (e.g. USB stick) may be used as the source. If no base station is paired, this function cannot be selected.
Name	Assigning a name to the base station (use only letters and digits, no special characters)
Remote Pairing	Configuration of the base station for remote pairing.

Press **Back** to navigate back to the main menu.

Fast response buttons

Pressing **Fast Response Buttons** takes you to the Fast Response Buttons menu.

The fast response buttons can be used to link the operating elements on the handheld device to the outputs of the base station.

KEBA © KEBA 2021

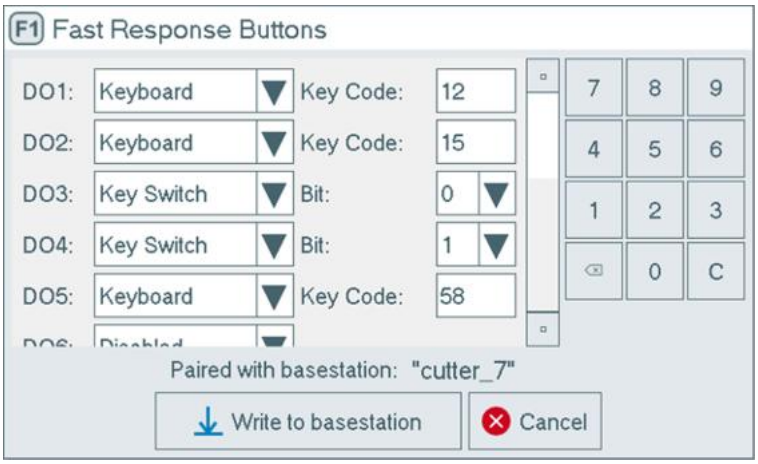


Fig. 8-77: Fast response buttons window

The following options for fast response buttons may be selected from the drop-down list.

Selection	Description
Auto-Detect	After the selection is made, either a button has to be pressed or a built-in element has to be actuated, e.g. the joystick has to be moved in some direction. The result of this action is applied.
Keyboard	The scan code of the key is used.
Key switch	The number of bits available depends on the hardware used.
Joystick	2 bits are used per axis.
Push button	1 bit
Push switch	1 bit
Rotary switch	The number of bits available depends on the hardware used.
Select switch	The number of bits available depends on the hardware used.
Disabled	The output is not used.

Write to base station transfers the settings to the base station and switches back to the previous window. **Cancel** leaves the window without saving the changed settings.

Name

Pressing **Name** takes you to the menu for assigning a name to the base station.

© KEBA 2021

Fig. 8-78: Assigning a name to the base station

Designation	Meaning
Name:	Assigning a name to the base station (no special characters allowed)

Write to base station transfers the settings to the base station and switches back to the previous window. Tap **Cancel** to exit the window without saving the changed settings.

Remote Pairing

Pressing **Remote Pairing** takes you to the menu for basic remote pairing settings.

In this dialog, the basic settings for using remote pairing can be configured.

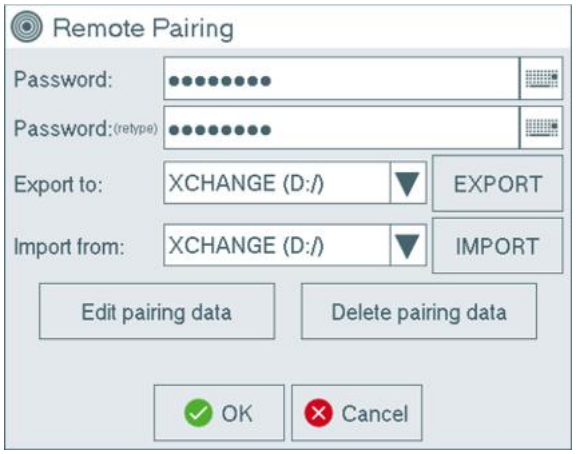


Fig. 8-79: Basic remote pairing settings

Designation	Meaning
Password	Assigning a password for using remote pairing later. Protects against improper use.

KEBA © KEBA 2021

Designation	Meaning
Export to	Exporting the list of base stations that the handheld device has previously been paired with. (During each pairing process, the identifier (MAC address and name) of the base station is stored in the paired handheld device.) This list can be used with the remote pairing function to select the base station.
Import from	Importing the list of base stations on the handheld device to enable selection of the base station by name when remote pairing is used.
Edit pairing data	Editing the list of base stations
Delete pairing data	Deleting the list of base stations

OK saves the settings and switches back to the previous window. **Cancel** leaves the window without saving the changed settings.

Information

*Pressing **Cancel** cannot undo imports of – or modifications to – connection data and cannot undo deletion of the connection data.*

Edit pairing data

Pressing **Edit pairing data** takes you to the list of remote pairing data.

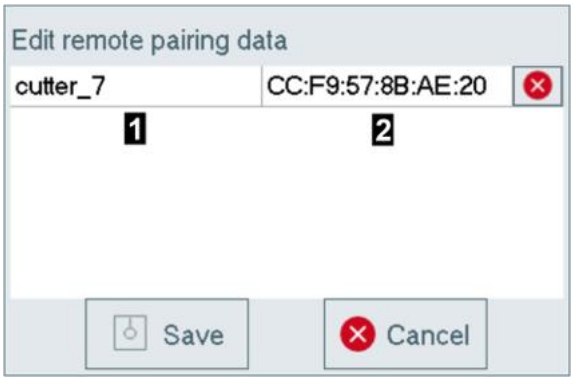


Fig. 8-80: List of remote pairing data

1 ... Name of the base station	2 ... MAC address of the base station

Pressing the red **X** right next to a connection can delete it from the list.

Save saves the settings and switches back to the previous window. **Cancel** leaves the window without saving the changed settings.

8.4.2 Diagnosis data

By pressing **Diagnosis Data**, you can save diagnostic data for the handheld device to a USB stick.

To do this, proceed as follows:

© KEBA 2021

1) Plug a USB stick into the handheld device.
2) Press **Diagnosis Data**.
3) In the dialog, select USB stick.

The diagnosis data is copied to the USB stick.

Information

Never remove a USB stick during the saving process! This may otherwise result in loss of data.

8.4.3 Display

Pressing "Display" calls up the display window.

Press "Back" to navigate back to the main menu.

Brightness

Press "Brightness" to display the screen for the brightness setting. The brightness of the display is adjusted with the slider.

Fig. 8-81: Brightness settings

Press "OK" to save the settings to the base station and switch back to the previous window. "Cancel" leaves the window without saving the changed settings.

Information

If the display brightness is set to more than 70 %, the performance of CPU and GPU is reduced, to prevent a rise of temperature inside the device.

Information

Carry out the calibration with a touch stylus.

KEBA © KEBA 2021

Press **Touch Calibration** to start touchscreen calibration. The following symbol is used for calibration:

For calibration, the symbol is displayed multiple times in succession in all 4 corners of the display. The order of the display is top left, top right, bottom left and bottom right. For each display of the symbol, the center of the symbol must be touched as precisely as possible. Care should be taken to select points only briefly - pressing too long will result in incorrect calibration.

After successful calibration, the calibration window is closed and the calibration of the touch screen is completed.

8.4.4 Licenses

Pressing **Licenses** will display the license terms.

OK exits the menu again.

8.4.5 Network

Tapping "Network" calls up the network window. In this window, the network settings for available Ethernet connections can be changed.

Fig. 8-82: Network window

Designation	Meaning
Base station connection	Network settings for the base station
Hall connection	Network settings for the hall network

© KEBA 2021

Designation	Meaning
Mode	Behavior between handheld device and base station

Tap "Back" to navigate back to the main menu.

Base station connection

Tapping "Base station connection" takes you to the menu for the base station.

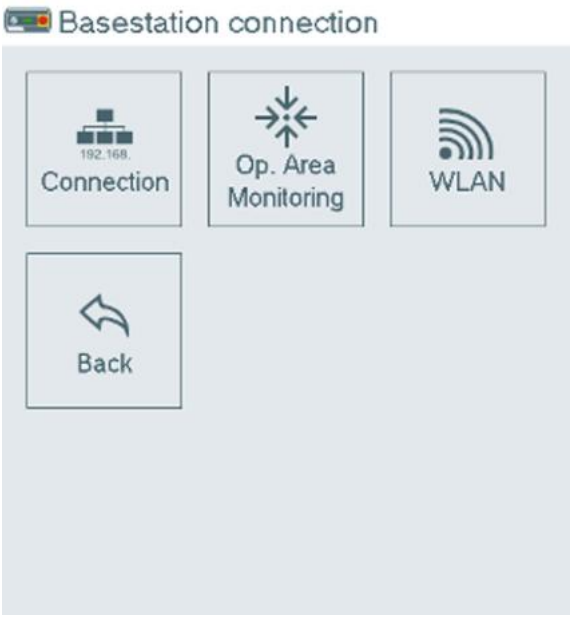


Fig. 8-83: Base station window

Designation	Meaning
Connection	Configuration of the base station network settings.
Op. Area Monitoring	Configuration of the operation area monitoring communications channel.
WLAN	Configuration of the generated wireless network between the base station and handheld device.

Tap "Back" to navigate back to the network window.

Connection

Tapping "Connection" takes you to the configuration window for base station network settings.

The network address can either be obtained automatically via DHCP or configured manually.

KEBA © KEBA 2021

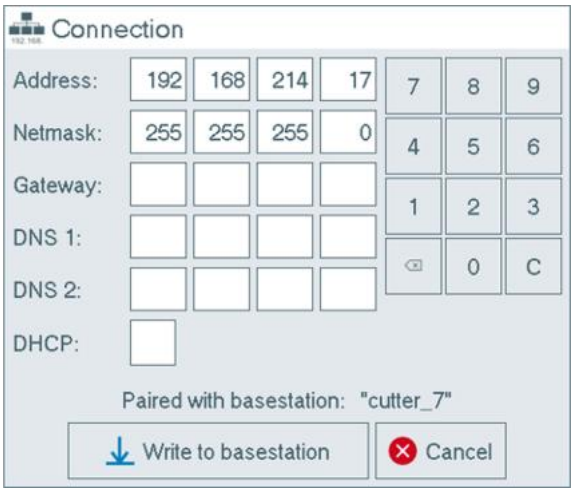


Fig. 8-84: Configuration of the network settings

Designation	Meaning
Address:	IP address of the handheld device
Net mask:	Associated subnet mask
Gateway:	Default gateway
DNS 1:	
DNS 2:	
DHCP:	

"Write to base station" transfers the settings to the base station and switches back to the previous window. Tap "Cancel" to exit the window without saving the changed settings.

Op. Area Monitoring

Tapping "Op. Area Monitoring" takes you to the configuration window for the operation area monitoring communications channel.

You can select the channel and wireless band for the operation area monitoring.

Information

To prevent interference, the channel selected for operation area monitoring must not be the same as the WLAN channel. Only the channel may be changed, however, not the wireless band.

If multiple devices with operation area monitoring are operated in parallel, it is likewise necessary to use different communications channels. In an area of 500 m², no more than five active connections may be operated in parallel.

© KEBA 2021

Fig. 8-85: Configuration of operation area monitoring

Designation	Meaning
Band:	Frequency for operation area monitoring
Channel:	Channel for operation area monitoring

"Write to base station" transfers the settings to the base station and switches back to the previous window. Tap "Cancel" to exit the window without saving the changed settings.

WLAN

Tapping "WLAN" takes you to the configuration window of the generated WLAN between the base station and handheld device.

For this WLAN, the channel and the wireless band can be selected; all other WLAN parameters are defined automatically by the base station and shared with the handheld device.

Information

If operation area monitoring is used, the WLAN communication with the base station should be operated on the 5 GHz frequency band.

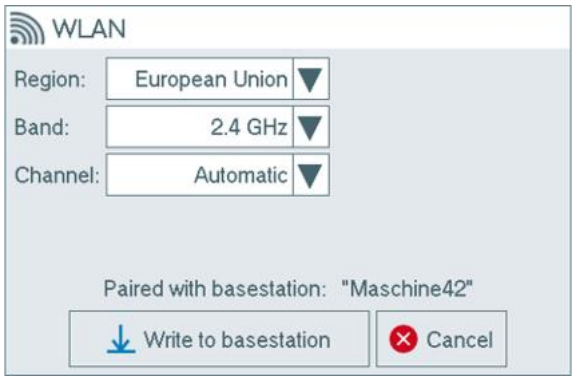


Fig. 8-86: WLAN settings

Designation	Meaning
Region:	Region in which the base station is operated

KEBA © KEBA 2021

Designation	Meaning
Band:	WLAN frequency
Channel:	WLAN channel

"Write to base station" transfers the settings to the base station and switches back to the previous window. Tap "Cancel" to exit the window without saving the changed settings.

Hall connection

Tapping "Hall connection" takes you to the configuration window for the hall network.

The network address can be configured in the following ways:

- DHCP: This enables automatic integration into an existing network without manual configuration.
- Manually: During this process, the individual four segments of the network addresses must be entered via the numeric input panel (select corresponding segments).

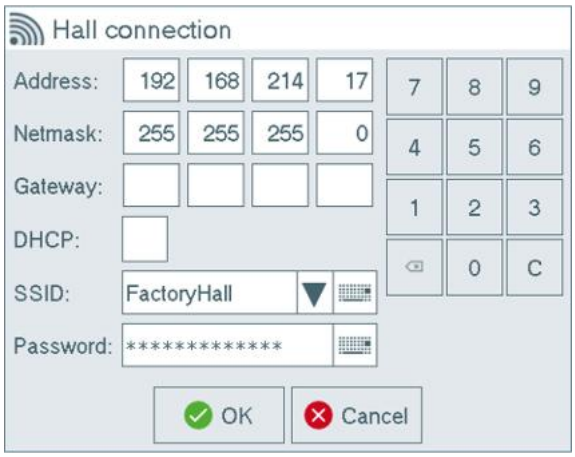


Fig. 8-87: Configuration of the hall network

Designation	Meaning
Address:	IP address of the handheld device
Net mask:	Associated subnet mask
Gateway:	Default gateway
DHCP:	Through the activation of "DHCP", the IP address will be automatically obtained via a DHCP server and the remaining input lines will be deactivated.
SSID:	SSID of the WLAN (you can select one from the list of received WLANs).
Password	Password of the WLAN

© KEBA 2021

Mode

Tapping "Mode" takes you to the parameter menu.

These parameters can be used to define the behavior of the handheld device with the base station.

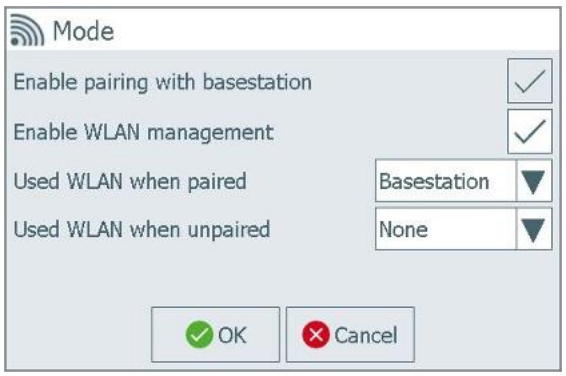


Fig. 8-88: Parameter settings

Designation	Meaning
Enable pairing with base station	Allow pairing (establishment of a secure connection) between handheld device and base station
Enable WLAN management	Activation of WLAN detection. No connection to a WLAN is possible without selection.
Used WLAN when paired	Selection of the WLAN with which the handheld device connects in the paired state: ● Base station: Base station ● Hall: Hall network ● None: not applicable
Used WLAN when unpaired	Selection of the WLAN with which the handheld device connects as soon as the secure connection to the base station is disconnected. ● Hall: Hall network ● None: not applicable

"OK" saves the settings and switches back to the previous window. Tap "Cancel" to exit the window without saving the changed settings.

Also see about this

Intended use [▷ 14]

8.4.6 Reboot

Press **Reboot** to restart the handheld device.

8.4.7 Shutdown

Pressing **Shutdown** shuts down the handheld terminal.

KEBA © KEBA 2021

8.4.8 Version info

Pressing "Version info" displays version information about installed software components:

- Windows base image
- BIOS
- Basestation bootloader (when connected to a base station)
- Basestation firmware (when connected to a base station)
- Baseboard OpControl bootloader
- Baseboard OpControl firmware

Fig. 8-89: Version information

Use **OK** to leave the window.

Information

The number of version information listed may differ depending on the equipment of the handheld terminal or base station.

8.5 PROFINET configuration (only for CB42x)

Information

Before the configuration, the GSDML file of the CB42x must be loaded into the project planning tool being used. The file can be downloaded from the KEBA data portal.

The following entries must be made for the gateway module during the PROFINET configuration:

Safety parameters

© KEBA 2021

Parameter	Description
F_SIL	SIL1; SIL2; SIL3
F_Source_Add	Specifies the F-address of the host (dec)
F_Dest_Add	Specifies the F-address of the CB42x (dec)
F_WD_Time	Watchdog time of the CB42x The value can be set between 50 ms and 2000 ms. We recommend not setting the watchdog time under 100 ms.

The gateway module does not support iParameter. iParameters can neither be set with the used project planning tool nor with any other method.

PROFINET RT Config

The "Update Time" parameter for the PROFINET Cycle Time must not be below 4 ms.

8.5.1 Process data image

Slot 1: System status

Input data

Bit	Name	Type	Address	Description
Bit 0	Connected	BOOL	%I X.0	0 = No secure connection between handheld device and base station 1 = Connection between handheld device and base station
Bit 1-7			%I X.1 - 7	reserved

Output data

None.

Slot 2: Safety PDU PROFIsafe

Input data

Bit	Name	Type	Address	Description
Bit 0	Enabling switch	BOOL	%I X.0	1 = "Enable" position
Bit 1	Panic enabling switch	BOOL	%I X.1	0 = "Panic" position
Bit 2	Emergency stop	BOOL	%I X.2	1 = "Unlocked" position
Bit 3	Pairing	BOOL	%I X.3	1 = KeTop is connected in "Standard Pairing" mode
Bit 4	Remote Pairing	BOOL	%I X.4	1 = KeTop is connected in "Remote Pairing" mode
Bit 5	WAL3	BOOL	%I X.5	1 = KeTop is in WAL Zone 3 (infringement area)
Bit 6	WAL2	BOOL	%I X.6	1 = KeTop is in WAL Zone 2 (tolerance range)

KEBA © KEBA 2021

Bit	Name	Type	Address	Description
Bit 7	WAL1	BOOL	%I X.7	1 = KeTop is in WAL Zone 1 (operation area)

Enabling switch process data

System state	Value bit 0	Value bit 1
Enabling switch "not pressed"	0	1
Enabling switch "pressed"	1	1
Enabling switch "panic"	0	0

Emergency stop process data

System state	Value bit 2
Emergency stop "pressed"	0
Emergency stop "unlocked"	1

Pairing mode process data

System state	Value bit 3	Value bit 4
No handheld device connected	0	0
"Standard Pairing" handheld device	1	0
"Remote Pairing" handheld device	0	1

Operation area process data

System state	Value bit 5	Value bit 6	Value bit 7
No operation area configured / no KeTop connected to base station	0	0	0
Handheld device in the work area	0	0	1
Handheld device in the warning area	0	1	0
Handheld device in the infringement area	1	0	0

Output data

None.

Information

In the unpaired state, bit 1 is in state 0 (= "Panic" position). Only use a paired handheld device to evaluate bit 1.

In safe state, the whole process data image equals "0".

Slot 3: Keyboard

One bit corresponds to one pressed key. The keyboard mapping is found on the version data sheet for the device.

© KEBA 2021

Input data

Byte	Name	Type	Address	Description
1-4	Keyboard	DWORD	%IDW X	Keyboard mapping according to version data sheet

Output data

Byte	Name	Address	Description
1	LED	%QB X	LED 1-8 ON/OFF
2	LED blink	%QB X+1	LED 1-8 blinking

Slot 4: Operator control elements

Input data

Byte	Name	Type	Address	Description
1	Switching element 1	Byte	%IB X	State of switching element 1
2	Switching element 2	Byte	%IB X+1	State of switching element 2

Output data

Byte	Name	Address	Description
1	Signal output switching element 1	%QB X	LED 1-8 ON/OFF
2	Signal output switching element 2	%QB X+1	LED 1-8 blinking

Slot 5: Hand wheel

Input data byte 0-1

Byte	Name	Type	Address	Description
Byte 0-1	Handwheelcounter	WORD	%IW X+1	Handwheelcounter

Input data byte 2

Bit	Name	Type	Address	Description
Bit 1	Handwheel pushbutton	BOOL	%I X +2.0	Hand wheel pressed
Bit 2-8			%I X	reserved

Output data

None.

KEBA © KEBA 2021

8.6 EtherCAT / FSoE configuration (only for CB43x)

Information

Before the configuration, the ESI-XML file must be loaded into the project planning tool being used.

The ESI-XML file is of XML format and contains the complete device properties of an EhterCAT slave. It also contains information about the EtherCAT or FSoE master: functions, settings and the process data image.

The following entries must be made for the gateway module during the EtherCAT / FSoE configuration:

Safety parameters

Parameter	Description
F_SIL	SIL1; SIL2; SIL3
F_Source_Add	Specifies the F-address of the host (dec)
F_Dest_Add	Specifies the F-address of the CB43x (dec)
F_WD_Time	Watchdog time of the CB43x The value can be set between 50 ms and 2000 ms. We recommend not setting the watchdog time under 100 ms.

FSoE cycle time

It is recommended to use an FSoE cycle time of 100 ms.

8.6.1 Process data image

Keyboard input data

One bit corresponds to one pressed key. The keyboard mapping is found on the version data sheet for the device. The addresses depend on the EtherCAT configuration.

KBI	Name	Type	Address	Description
0 - 31	Keyboard	BIT	%Qxx.xx	Keyboard mapping according to version data sheet

Keyboard output data (LEDs)

Byte	Name	Type	Address	Description
1	ON0-7	BYTE	%Qxx.xx	LED 1 - 8 on/off
2	BLINK0-7	BYTE	%Qxx.xx	LED 1 - 8 blinking

© KEBA 2021

Push buttons output data

Value	Name	Type	Address	Description
ON0-3	LED on	4-BIT	%Qxx.xx	Push button LED 1 - 4 on
BLINK0-3	Operator control 2	4-BIT	%Qxx.xx	Push button LED 1 - 4 blinking

Modul 1 (FSoE)

Enabling switch process data

System state	Value bit 0	Value bit 1
Enabling switch "not pressed"	0	1
Enabling switch "pressed"	1	1
Enabling switch "panic"	0	0

Emergency stop process data

System state	Value bit 2
Emergency stop "pressed"	0
Emergency stop "unlocked"	1

Pairing mode process data

System state	Value bit 3	Value bit 4
No handheld device connected	0	0
"Standard Pairing" handheld device	1	0
"Remote Pairing" handheld device	0	1

Operation area process data

System state	Value bit 5	Value bit 6	Value bit 7
No operation area configured / no KeTop connected to base station	0	0	0
Handheld device in the work area	0	0	1
Handheld device in the warning area	0	1	0
Handheld device in the infringement area	1	0	0

Output data

None.

Information

In the unpaired state, bit 1 is in state 0 (= "Panic" position). Only use a paired handheld device to evaluate bit 1.

In safe state, the whole process data image equals "0".

KEBA © KEBA 2021

Working counter state

Value	Name	Type	Description
WcState	Working counter state	BIT	0 = valid real time communication in latest cycle 1 = invalid real time communication

System state (InfoData)

Value	Name	Type	Address	Description
State	EtherCAT state	UINT		0x____1 = slave in state "INIT" 0x____2 = slave in state "PREOP" 0x____3 = slave in state "BOOT" 0x____4 = slave in state "SAFEOP" 0x____8 = slave in state "OP" 0x001_ = slave signalizes error 0x002_ = invalid "vendorId, productCode...read" 0x004_ = initialization error occurred 0x008_ = slave shut down

8.7 Configure hibernation

The start-up behavior from the idle state can be configured using the DIP switch in the connection slot of the handheld terminal (see 4.6.1 Cable entrance area).

Switch position OFF (default setting)

If the switch is in position "STBY_OFF", a fast start-up of the handheld terminal is not possible. In the idle state, the CPU is no longer supplied with power. This allows a longer battery life (approx. 15 days).

Switch position ON

If the switch is in position "STBY_ON", a fast start-up and recovery of the last state ("Suspend to RAM") is possible. The CPU continues to be supplied with power in the idle state. This shortens the battery runtime (to approx. 2 days).

© KEBA 2021

8.8 Remote access to KeTop

Information

The standard configuration is active on the device. Remote access from outside (such as the "ping" function) is deactivated.

The following description is valid for handheld devices with Windows 10 only.

Using the setup "WindowsCustomizingSetup", different remote access services can be activated.

Safety information

Due to the possibility of unauthorized access to the device, activating remote access is an IT security risk.

The following services can be activated:

- Remote desktop (RDP): This service enables access to the device via a remote desktop client.
- Server Message Block file sharing (SMB): This service enables access to the device via approved folders.
- ICMP (for ping): This service makes it possible to check the Ethernet connection to the device by "pinging".
- KeStudio: This service creates firewall rules that enable the use of KeStudio.

Installation

In order to install a service, proceed as follows:

1) Call up the setup using "Programs and Functions" - "WindowsCustomizingSetup".
2) Click on "Change".
3) Select the desired service.

Service	Setup name
Remote desktop	`RDP activation`
Server Message Block File Sharing	`SMB activation`
ICMP	`PING activation`
KeStudio	`KeStudio activation`

4) Click on the black selection arrow next to the selected service.
5) Select "Entire Feature will be installed on local hard drive".
6) Click on "Next" - "Change" - "Finish" to complete the installation.

KEBA © KEBA 2021

Uninstallation

In order to uninstall a service, proceed as follows:

1) Call up the setup using "Programs and Functions" - "WindowsCustomizingSetup".
2) Click on "Next" - "Change".
3) Select the service to be uninstalled.
4) Click on the black selection arrow next to the selected service.
5) Select "Entire feature will be unavailable".
6) Click on "Next" - "Change" - "Finish" to complete the uninstallation.

8.8.1 Remote Access via OpenSSH

OpenSSH enables secure remote access to the T15xWL via the SSH protocol. The OpenSSH server is not installed on the device by default and can be installed via the Windows settings

Installation

To install the OpenSSH server, proceed as follows:

1) Open the Windows settings using the Windows key + I key combination or via the Start menu.
2) Navigate to System.
3) Select Optional features.
4) Select Add a feature.
5) Enter OpenSSH in the search field.
6) Select OpenSSH Server from the list.
7) Select Install (Add).

The OpenSSH server is installed.

Access to the OpenSSH server is provided via TCP port 22, provided that no restrictions are caused by firewall rules.

Information

An active internet connection is required to install the OpenSSH server. The feature is obtained via the optional Windows features.

Uninstallation

To uninstall the OpenSSH server, proceed as follows:

1) Open the Windows settings using the Windows key + I key combination or via the Start menu.
2) Navigate to System ► Optional features.
3) Search for OpenSSH Server in the list of installed features.

© KEBA 2021

4) Select Remove.

The OpenSSH server is uninstalled.

8.9 Security settings

The following security settings are available:

- Whitelisting using AppLocker
- Kiosk Desktop
- KEBA Write Filter

No applications are already installed at the time of delivery.

Whitelisting using AppLocker

AppLocker allows the execution of programs which are registered in the list (whitelist) and stored with execution rules to be blocked.

Kiosk Desktop

Adjusting the operating system offers you the ability to restrict the user access right to the KeTop.

KEBA Write Filter

Installing this function protects the file system with the KEBA Write Filter.

Information

Once KeWF is active, no setup can be executed. KeWF must be stopped manually (by an administrator) in order to make a change through a setup. The KeWF feature itself also cannot be deinstalled while the write filter is active.

To stop KeWF manually, open a Command Prompt and execute the following command:

```
net stop KeWF <enter>
```

8.9.1 (Un-) installation

No components of the security setup are already installed at the time of delivery.

Installation

In order to install a service, proceed as follows:

1) Call up the setup using "Programs and Functions" - "WindowsSecurity-Setup".
2) Click on "Change".

KEBA © KEBA 2021

3) Select the desired service.
4) Click on the selection arrow next to the selected service - "Entire Feature will be installed on local hard drive".
5) Click on "Next" - "Change" - "Finish" to complete the installation.

The respective service is installed and will become active after a restart.

Uninstallation

In order to uninstall a service, proceed as follows:

1) Call up the setup using "Programs and Functions" - "WindowsSecurity-Setup".
2) Click on "Change".
3) Select the desired service.
4) Click on the selection arrow next to the selected service - "Entire Feature will be unavailable".
5) Click on "Next" - "Change" - "Finish" to complete the uninstallation.

After a restart, the respective service is uninstalled and all settings are reset.

8.9.2 Whitelisting using AppLocker

AppLocker blocks the execution of programs, scripts and installation programs if they are not registered in a list (whitelist) and stored with execution rules.

These rules are stored in the default settings for the users (excluding admins).

Exceptions are defined by default for the following folders:

- %ProgramFiles%
- %ProgramFiles(x86%)
- Windows folder

The standard configuration allows the standard user to run programs from the excluded directories.
Administrators, on the other hand, can run all programs.

The configuration of AppLocker can be adjusted after installation using a local security policy (secpol.msc).

More information on the configuration, as well as a detailed description of AppLocker, can be viewed on the Microsoft© homepage.

8.9.3 Kiosk Desktop

User access to the device can be restricted using Kiosk Desktop. This can be used, for example, as protection against operating errors.

The Kiosk Configurator is used to configure the Kiosk Desktop. This is available on the desktop as a shortcut after installation.

© KEBA 2021

Information

When the configuration has been completed, the kiosk desktop is always displayed after starting the device.

Kiosk Configurator

The interface of the Kiosk Configurator consists of the following tabs:

- Settings: Making visual adjustments
- Shortcuts: Editing links
- Blocked keys: Defining blocked keys/key combinations
- Colors: Setting background and text colors
- Dock: Editing shortcuts on the taskbar
- Action: Restarting, importing, exporting

Settings

Under "Settings," the graphics for the logo, header and footer can be replaced and the positions of shortcuts can be configured.

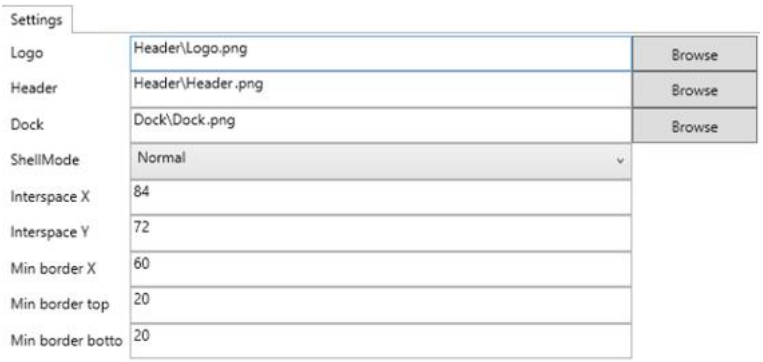


Fig. 8-90: "Settings" tab

Name	Description
Logo	Insert logo graphic in the top right using "Browse"
Header	Insert graphic in the header using "Browse"
Dock	Insert graphic in the footer using "Browse"
Shell Mode	Level of the Kiosk Desktop (can be selected in the drop-down menu)
Interspace X	X distance between shortcuts
Interspace Y	Y distance between shortcuts
Min border X	Minimum distance to borders
Min border top	Minimum distance upward
Min border bottom	Minimum distance downward

KEBA © KEBA 2021

Shortcuts

Under "Shortcuts," links (shortcuts) can be created and managed.

All shortcuts created are listed in the left column. These are created using "New file" and "New dir".

The shortcuts which appear on the desktop are listed in the right column.

If one graphic for the normal display state and another graphic for the print state are stored for a shortcut, the shortcut is immediately set to active and is visible on the Kiosk Desktop.

The order of elements can be adjusted with "▲" and "▼".

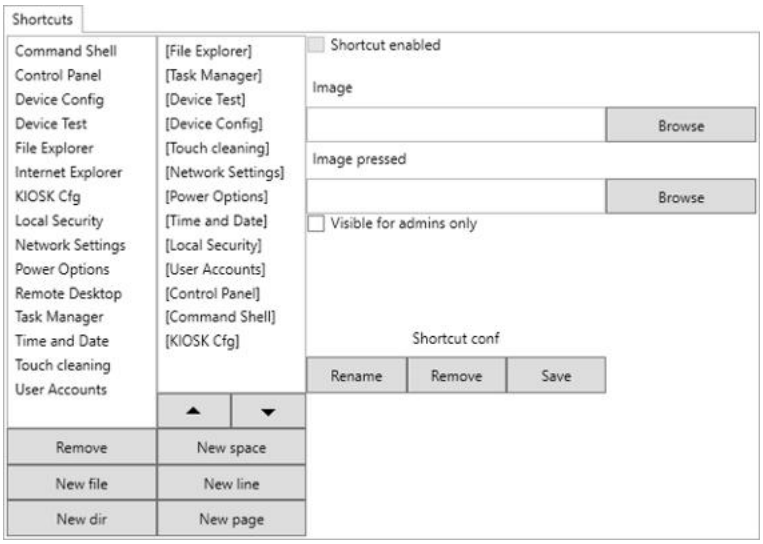


Fig. 8-91: "Shortcuts" tab

Name	Description
Remove	Deleting a shortcut
New file	Creating a new file shortcut
New dir	Creating a new folder shortcut
▲	Moving a selected element up (forward)
▼	Moving a selected element down (backward)
New space	Inserting an empty space
New line	Beginning a new line
New page	Beginning a new page
Shortcut enabled	Shortcut is active (set automatically if both graphics are stored)
Image	Inserting a graphic using "Browse"
Image pressed	Inserting a graphic for the printed state using "Browse"
Visible for admins only	Shortcut only visible for admins
Rename	Renaming the shortcut

© KEBA 2021

Name	Description
Remove	Deleting a shortcut
Save	Saving the configuration

Blocked keys

Under "Blocked keys", keys and key combinations can be blocked.

Elements are displayed in the left column (maximum 8) to which blocked keys can be added. The respective added (blocked) keys are displayed in the right column.

By selecting one of the elements from the left column, the blocked keys can be selected in the drop-down menu and added to the element using "Add key".

Fig. 8-92: "Blocked keys" tab

Name	Description
Key	Drop-down menu with all available keys
Add key	Blocking selected key
Remove keys	Removing selected key

Colors

Under "Colors," the colors of the Kiosk Desktop can be adjusted.

Using "Select," the desired color can be selected. The RGB values of the selected color are displayed in the colored fields.

KEBA © KEBA 2021

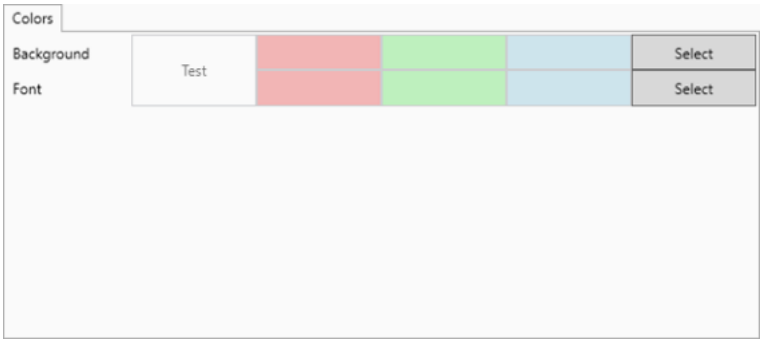


Fig. 8-93: "Colors" tab

Name	Description
Background	Background color
Font	Font color

Dock

Under "Dock," certain functions can be attached to the taskbar.

Shutdown, Restart, Tasks, Lock, Logout and OSK (On Screen Keyboard).

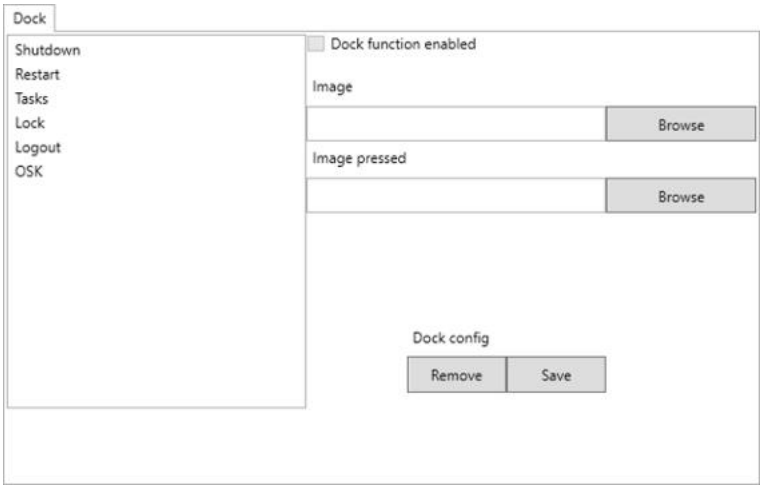


Fig. 8-94: "Dock" tab

Name	Description
Image	Inserting a graphic using "Browse"
Image pressed	Inserting a graphic for the printed state using "Browse"
Remove	Removing the function
Save	Saving the function

Action

Under "Action," the Kiosk Desktop can be set as a start application (Active shell), restarted or the configuration can be exported and imported.

© KEBA 2021

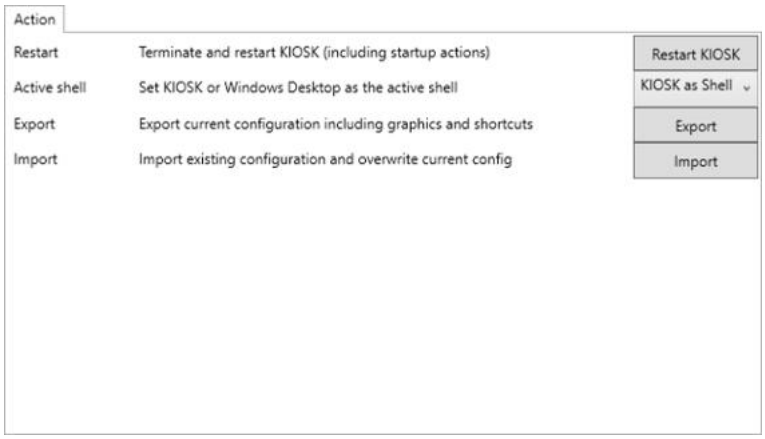


Fig. 8-95: "Action" tab

Name	Description
Restart	Restarts the Kiosk Desktop Changes to the configuration are only visible after restarting
Active shell	
• KIOSK by ShellLauncher	Kiosk Desktop is run automatically upon start up (only available with Windows 10 or higher) All programs in auto start are run. Only select in consultation with KEBA.
• KIOSK as Shell	Kiosk Desktop is run upon start up (selected as standard) All programs in auto start are run.
• Explorer	Deactivates the automatic start of Kiosk Desktop
Export	Export of the configuration (incl. Kiosk Desktop folder)
Import	Import of a configuration

8.9.4 KEBA Write Filter

Installing this function protects the file system with the KeWF (KEBA Write Filter).

The standard configuration prevents files with the following file extensions on the C:\ drive from being created, renamed or deleted (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
*.cmd, *.chm, *.com, *.cpl, *.crt	*.job, *.js, *.jse, *.jar	*.u3p, *.url
*.docm, *.dotm, *.dll	*.lnk	*.vb, *.vbe, *.vbs, *.vbscript

KEBA © KEBA 2021

a - g	h - p	m - z
*.exe, *.ex_	*.msc, *.msi, *.msp, *.mst	*.ws, *.wsf, *.wsh
*.gadget	*.paf, *.pif, *.ps1, *.pyc, *.pyo, *.pnf	*.xml

On all other drives, files with the extensions listed can still be created, renamed and deleted.

In the configuration, other exceptions (Whitelist) and "Wildcards" can be defined and additional drives protected. In the standard configuration, the exception applies to the following files: "pagefile.sys" and "hiberfil.sys"

Example: While all *.exe and *.dll files can be blocked using the "Blacklist," at the same time, the `C:\Kundenverzeichnis1\*.exe` and `C:\Kundenverzeichnis2\KundenLibrary.dll` paths can be allowed using the "Whitelist".

Information

For further information on configuring KeWF, please contact KEBA support.

8.10 Connectivity protocols

In order to transmit data between the handheld device and the control, a protocol must be defined. The following protocols are supported:

- KVC: Defined, proprietary protocol from KEBA integrated into the control.
- Modbus: Open standard
- OPC UA: Open standard
- ADS: Standard protocol for Beckhoff devices
- S7: Standard protocol for Siemens devices

By default, a protocol is not activated in delivery condition. More information can be found in the respective protocol descriptions.

The connection protocols make it possible to transmit the following content from the handheld device to the control:

- Transmission of state changes of keys on the keypad or of operating elements
- Setting and reading LED states
- Control of the handheld device or transfer of various parameters

© KEBA 2021

Information

It is possible to use different connection protocols for the individual transmissions. We recommend using only one connection protocol, because otherwise, the protocols will interfere with each other.

Installation

Information

The Windows platform driver setup may be used only for the installation of a connection protocol. Installing another device is not permitted and can cause malfunctions during operation.

In order to install a connection protocol, proceed as follows:

1) Call up the setup using "Programs and Functions" - "WindowsPlatformDriverSetup".
2) Click on "Next" - "Change".
3) Select the desired protocol.

Protocol	Setup name
KVC	`KEBA Virtual Channel`
Modbus	`ModbusItf`
OPC UA	`OPCUAItf`
ADS	`ADSItf`
S7	`S7Itf`

4) Click on the black selection arrow next to the selected protocol.
5) Select "Entire Feature will be installed on local hard drive".
6) Click on "Next" - "Change" - "Finish", to complete the installation.

Uninstallation

In order to uninstall a connection protocol, proceed as follows:

1) Call up the setup using "Programms and Functions" - "WindowsPlatformDriverSetup".
2) Click on "Next" - "Change".
3) Select the protocol to be uninstalled.
4) Click on the black selection arrow next to the selected protocol.
5) Select "Entire feature will be unavailable".
6) Click on "Next" - "Change" - "Finish", to complete the uninstallation.

KEBA © KEBA 2021

8.11 Key management

For each key, there is a predefined key code. Key mapping makes it possible to modify or disable the predefined key codes so that they are no longer evaluated in Windows.

The PS/2 code of the corresponding button can be determined using the “DeviceTestTool”.

Key mapping configuration

To assign a function (output) to the keys of the keypad on the handheld device, the keys must first be integrated. To do this, proceed as follows:

1) Open the `WinKeyMapExample.cfg` file in the `C:\ProgramData\KEBA Automation\keview\system` directory with an editor.

Information

The `C:\ProgramData` directory is hidden by default and must be made visible via the Explorer display settings

2) Copy all entries to the `[ScancodeMapping_Txxx_Standard]` or `[ScancodeMapping_Txxx_Robotic]` subitem.
3) Add all entries to the `[ScancodeMapping]` subitem.

The keys of the keypad can then be assigned the desired output as follows.

Keypad key = keypad key code*), modifier*), desired output, desired modifier

* This setting may not be changed.

Example:

```
KEY_001 = 00,20, 00,00,00,00,00,00, 00,3B, 00,2A,00,00,00,00
```

Then, the file must be saved as `KeyMap.cfg` in order to apply the changes. The date and time are attached to the file name automatically (after a short time).

A list of available key codes and modifiers for the output can be found in the following chapter.

Disabling key functions

In order to disable all key functions, proceed as follows:

1) Open the `WinKeyMapExample.cfg` file.
2) In the `[Settings]` subitem, set the following parameter to 1: `DropAllKeys=1`
3) Save the file as `KeyMap.cfg` in the `C:\ProgramData\KEBA Automation\keview\system` directory. The date and time are attached to the file name automatically (after a short time).

© KEBA 2021

8.11.1 Key codes

The following tables contain the available PS/2 codes (set 1) in hexadecimal notation.

Modifiers

Key	PS/2 code	Key	PS/2 code
Left Ctrl	00 1D	Right Ctrl	E0 1D
Left Shift key	00 2A	Right Shift key	00 36
Left Alt	00 38	Right Alt	E0 38
Left Windows key	E0 5B	Right Windows key	E0 5C

Keys (referring to an English keyboard layout)

Key	PS/2 code	Key	PS/2 code
' "	00 28	Number pad -	00 4A
, <	00 33	Number pad . Delete	00 53
- _	00 0C	Number pad /	E0 35
. >	00 34	Number pad 0 Ins	00 52
/ ?	00 35	Number pad 1 End	00 4F
0)	00 0B	Number pad 2 down	00 50
1 !	00 02	Number pad 3 Pg Dn	00 51
2 @	00 03	Number pad 4 left	00 4B
3 #	00 04	Number pad 5	00 4C
4 $	00 05	Number pad 6 right	00 4D
5 %	00 06	Number pad 7 Home	00 47
6 ^	00 07	Number pad 8 up	00 48
7 &	00 08	Number pad 9 Pg Up	00 49
8 *	00 09	Number pad =	00 59
9 (	00 0A	Number pad Enter	E0 1C
; :	00 27	Num Lock	00 45
= +	00 0D	Page Down	E0 51
Down arrow	E0 50	Page Up	E0 49
Left arrow	E0 4B	Print Screen	E0 37
Right arrow	E0 4D	Enter	00 1C
Up arrow	E0 48	Scroll Lock	00 46
Backspace	00 0E	Space bar	00 39
Caps Lock	00 3A	Tab	00 0F
Delete	E0 53	[{	00 1A
End	E0 4F	\ |	00 2B
Esc	00 01	] }	00 1B
F1	00 3B	` ~	00 29

KEBA © KEBA 2021

Key	PS/2 code	Key	PS/2 code
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
Insert	E0 52	y Y	00 15
Number pad *	00 37	z Z	00 2C
Number pad +	00 4E		

8.12 Windows settings

Keyboard layout

The English keyboard layout is set by default on the handheld device. The user can add new keyboard layouts or select the primary language using the system control. For details on the settings, see the Microsoft© website.

Windows activation

WES7

The KeTop with WES7 is already delivered licensed and activated.

© KEBA 2021

Windows 10

The KeTop is delivered with a valid license and deferred activation. A product key of type Embedded Product Key Entry Activation (ePKEA) is integrated. Once the KeTop is connected to the Internet, activation takes place automatically. If the device is never connected to the Internet, it remains in the state of deferred activation. If activation fails and the device transitions to the "not activated" state, please contact KEBA.

For further information, see the Microsoft© website.

AutoLogon

With AutoLogon activated, a logon screen is not displayed on the handheld device after start-up. A password does not have to be entered.

Information

Complete start-up no longer possible!

If AutoLogon is activated, the user, user password and domain name may not be changed. To change these settings, AutoLogon must be deactivated.

Interrupt AutoLogon

To interrupt the automatic logon once, one of the shift keys must be pressed and held before Windows automatically logs on the configured user.

Write protection for storage media

WES7

Write protection for the memory can be implemented using the Enhanced Write Filter (EWF).

Windows 10

Write protection for storage can be implemented with Unified Write Filter (UWF).

For further information, see the Microsoft© website.

Windows key

The power key ⏻ corresponds to the Windows power key and can be assigned correspondingly. For details on the assignment, see the Microsoft© website.

Installing Microsoft Edge

Using the setup "WindowsCustomizingSetup", Microsoft Edge can be installed and set as default browser. To do so, proceed as follows:

1) Call up the setup using "Programs and Functions" - "WindowsCustomizingSetup".

KEBA © KEBA 2021

2) Click on "Change".
3) Select "Microsoft Edge".
4) Click on the black selection arrow next to the selected service.
5) Select "Entire Feature will be installed on local hard drive".
6) Click on "Next" - "Change" - "Finish" to complete the installation.

Activating additional ciphers

Using the setup "WindowsCustomizingSetup", additional ciphers that are required for WinCC can be activated. To do so, proceed as follows:

1) Call up the setup using "Programs and Functions" - "WindowsCustomizingSetup".
2) Click on "Change".
3) Select "Additional ciphers activation".
4) Click on the black selection arrow next to the selected service.
5) Select "Entire Feature will be installed on local hard drive".
6) Click on "Next" - "Change" - "Finish" to complete the installation.

8.13 Programming

HWApi

The handheld device features the HWApi programming interface, which can be used to address the operating elements and keyboard and query hardware properties. The HWApiSDK programming environment is required in order to use the HWApi programming interface. This can be obtained from KEBA on request.

For more information, please contact KEBA.

© KEBA 2021

9 Operation and handling

9.1 Start-up

The start-up or starting procedure of the handheld device after pressing the power key can be followed on the screen and proceeds in the following order:

1) Display of the boot splash screen
2) Loading and starting of the operating system. This procedure may take up to 3 minutes. A black screen is displayed during this time.
3) Login dialog (not shown if Autologon is activated)
4) Windows desktop is started

When first logging on with the "keba" administrator user, there is no need to enter a password. Immediately after the initial login, a password must be assigned. To do so, please follow the instructions on the monitor.

Caution

A flash storage media permits a limited number of write cycles. Once this limit has been reached, there is the risk of a hardware fault. We therefore recommend that you use an exchangeable storage medium for cyclical writing procedures (e.g. logging).

Standard user

The following default users are available on the device:

- keba: This user has **administrator rights** and can make system changes and install software.
- operator: This user has **standard rights** and is intended for normal operation without administrative privileges.

It is recommended to assign a different password for all users immediately after the first login in order to protect the system against unauthorized access. Please follow the instructions on the screen.

Information

In standard operation, the use of the "operator" user is recommended to ensure system security.

9.2 Shut down the KeTop

The device can be shut down using **Start ► Shut down**, for example. Appropriate concepts can be provided for the switch-off safety of the KeTop (e.g. UWF write filter, etc.).

KEBA © KEBA 2021

Power button

Pressing the power button ⏻ puts the KeTop into hibernation mode by default. The function of the power button can be configured using **Start ► Control Panel ► Power Options**.

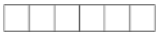
Caution

By default, the power button is configured so that when pressed (and held down), the device is disconnected from the power supply after 5 seconds. In this case, all data in the RAM of the device are lost.

9.3 Base station operating states

This chapter describes the possible operating states of the base station.

The currently active operating state is indicated via the LED status bar (or external signal column).

Display	Operating state	Description
Green	Normal	The handheld device is connected correctly and the emergency stop is not activated. The emergency stop outputs of the base station are in the same state as the emergency stop of the handheld device.
White 	Bridge active	The handheld device is not paired, the emergency stop outputs of the base station are closed, there is no invalid status, error or actuated emergency stop present when unpairing the handheld device.
White flashing	DIP switch not set	The DIP switch on the base station is not set. Set the DIP switch according to the table in the "Operating range configuration" chapter.
Yellow LEDs go out one after the other	Paring/Unpairing timer	A handheld device was paired with the emergency stop actuated. If the emergency stop is unlocked within approx. 10 seconds, the base station switches to a valid operating mode. If the time is exceeded, the base station switches to the safe state (the outputs are opened).

© KEBA 2021

Display	Operating state	Description
Red	Estop	Safe state. The following points can trigger the safe state: ● The emergency stop has been triggered on the handheld device or connection box. ● The "Reset" button on the base station was pressed. The handheld device was thus unpaired from the base station. The emergency stop must be unlocked to acknowledge this.

9.4 Operating behavior

Base station switched off

If the base station is switched off, the relays of the emergency stop circuits are no longer actively held closed and the emergency stop circuit is subsequently opened (comparable to activated emergency stop). The enabling switch outputs also remain open.

Base station switched on

If the base station is switched on (supplied with power), the states of the inputs and the last emergency stop state that was saved are retrieved. As a result of this query, the base station can take on the defined operating states. The enabling switch outputs remain open.

Operation with paired handheld device

After successfully pairing a handheld device to a base station, the emergency stop relay outputs of the base station follow the state of the emergency stop on the handheld device, as long as the emergency stop of the base station is not actuated. The enabling switch outputs follow the switching element on the handheld device.

It is not until after successfully establishing the secure connection between the handheld device and base station that the illuminated emergency stop of the handheld device becomes active. If an error at the base station causes the emergency stop on the handheld device to become disabled, but the operator receives the information that it is enabled, then the enabling switch outputs and the emergency stop outputs are opened.

If the base station is switched off with the handheld device paired, an error message is output on the handheld device. The handheld device must be restarted in order to enable proper operation (not paired).

KEBA © KEBA 2021

Operation with unpaired handheld device

If a handheld device is unpaired, the illuminated emergency stop on that device becomes inactive and the enabling switch is no longer functional. However, as an unpaired inactive emergency stop button does not trigger the "emergency stop" safety function, the emergency stop circuits of the base station remain closed. Thus the emergency-stop output (relay output) of the base station is not triggered. The other emergency stops present on the machine do not lose their effect.

If the secure connection between the handheld device and the base station is interrupted due to a fault or error, the emergency stop is automatically triggered at the base station.

An emergency stop triggered on the base station is not canceled by unpairing the handheld device.

Pairing/unpairing handheld device

If a handheld device is paired to the base station and if a different handheld device is to be paired, the currently paired device must be unpaired. (See 11 Pairing to base station.)

The illuminated emergency stop on the paired handheld device is activated after successful pairing to the base station.

If a handheld device with an activated emergency stop is paired, this emergency stop can be unlocked within 10 seconds without triggering an emergency stop. If the emergency stop is not unlocked within 10 seconds, an emergency stop is triggered.

9.5 Charging behavior of the battery

The battery can be charged using the charging station that is included in the scope of delivery. Optionally, use the power supply unit.

Charging at high ambient temperatures

During charging, computationally intensive applications at high ambient temperatures can lead to high temperatures of the battery.

If the ambient temperature exceeds 45°C, charging of the battery is interrupted. Charging will be continued, once the temperature of the battery drops below 40°C.

The following measures are recommended to cool down the battery:

- Bring the device into an environment with lower ambient temperature (< 25°C).
- Switch off the device for some time or switch to hibernation state.

© KEBA 2021

9.6 "System State" Dialog

If an additional battery (see 17.6 Zubehör) is plugged in, the icon of the "System State" display appears in the "System Tray" of the taskbar. Click on it or press the Ident button on the hand-held pendant station for at least 3 seconds to open the following dialog:

Fig. 9-96: "System State" dialog

Name	Description
WLAN:	WLAN connection
Battery:	Status of the internal battery
Battery Pack:	Status of the battery pack
Remote paring:	Establishing a secure connection (see 11 Pairing to base station)
OK	Close the dialog

KEBA © KEBA 2021

10 Validation

The following functions must be tested and documented once the base station has been wired up, installed and configured:

- Triggering the emergency stop of a connected handheld device
- Actuating and testing the switching elements, specifically the enabling switch and the key switch
- Carrying out and checking the entire pairing and unpairing process of the handheld device to/from the base station.
- If it is relevant to the application, carrying out and checking a remote pairing and unpairing process of the handheld device to/from the base station.
- Checking all safety functions (at a minimum, emergency stop and enabling switch)
- Checking the visibility/recognizability of an illuminated emergency stop as well as the LED bar and the signal column.

Information

For the validation, the machine must be in a safe state. The hazard area must be clear.

10.1 Validating the distance measurement

To display the distance measurement between the mobile handheld device and base station, proceed as follows:

- Perform the standard pairing of the handheld device with the base station.
- Press the "Ident" button for 3 seconds to open the "System State" dialog.
- Align the handheld device in direct visual contact with the base station.
- Move the handheld device to the boundary of the work area.
- Check whether the LED in the emergency stop switch pulsates at the expected distance value.
- Read the displayed distance value.

The displayed distance value must correspond to the actual distance with a tolerance of +/- 1 m.

© KEBA 2021

11 Pairing to base station

To establish a connection to the base station, "pairing" must be carried out between the handheld device and the base station. There can only ever be one handheld device paired with one base station. It is not until after successful "pairing" that the necessary configuration settings of the base station can be carried out (see 8.4.1 Base station).

The illuminated emergency stop is only functional if a proper connection to the base station is present. The secure data is transferred via Bluetooth, while the functional data is transferred via Wi-Fi. If the Bluetooth connection is interrupted, the emergency stop stops illuminating and is thus not available. Each time the connection is interrupted (e.g. due to exceeding the maximum distance from the base station), the devices remain paired. However, data transfer is now only possible over Wi-Fi (or not at all, depending on the distance).

If the handheld device is again within the Wi-Fi range of the base station, a secure Bluetooth connection to the originally paired base station is reestablished automatically. To pair the handheld device with a different base station, you must first unpair the handheld device from the originally paired base station.

Pairing the base station

To establish a secure connection ("pairing"), proceed as follows:

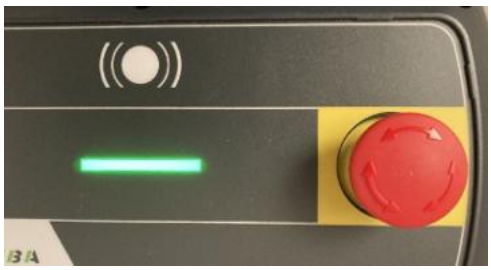
1) Hold the handheld device up to the desired base station (max. distance 2 cm).
2) When the base station is recognized, the device vibrates and a dialog opens automatically showing the serial number or name of the base station.
3) Confirm with "Yes".

The secure connection is established. You can tell the connection has been established successfully by the illumination status of the LED bar of the base station and the emergency stop of the handheld device. This must be verified using a visual inspection.

Information

If the optional operation area monitoring is configured, the user must be in the immediate vicinity of the base station until the pairing process is complete. Otherwise this can result in the machine coming to an undesired standstill.

KEBA © KEBA 2021

Base station connected	Handheld device connected
	

Depending on which configuration is set, the handheld device connects automatically to the base station or hall network for functional data exchange.

After the work is finished, the secure connection must be released by means of "unpairing".

Disconnecting the base station (unpairing)

To disconnect a secure connection ("unpair"), proceed as follows:

1) Hold the handheld device up to the desired base station (max. distance 2 cm).
2) The device vibrates and a dialog opens automatically showing the serial number or name of the base station.
3) Confirm with "Yes".

The secure connection is disconnected. You can tell the connection has been disconnected successfully by the illumination status of the LED bar of the base station and the emergency stop of the handheld device. This must be verified using a visual inspection.

Base station disconnected	Handheld device disconnected

Depending on which configuration is set, the handheld device connects automatically to the hall network for functional data exchange or remains offline.

Remote Pairing / Unpairing

WARNING!

It must be ensured that during a remote pairing, there is a permanently wired emergency stop in the vicinity of the user!

© KEBA 2021

If it is not possible in special operating modes or certain states to hold the handheld device directly up to the base station, the "Remote Pairing" function must be used. For this purpose, however, it is necessary for there to be a clear line of sight to the desired base station in order to ensure that the connection is actually to the desired base station.

Information

Before a Remote Pairing can be carried out, a pairing must have been carried out between the handheld device and base station, followed by a basic configuration.

We recommend connecting a handheld device to all base stations of a hall once in order to create a list of all base stations (refer to the 8.4.1 Base station) chapter. This list can be transmitted using "Export" on the original handheld device and "Import" on all other handheld devices to make the remote pairing/unpairing easier.

Remote Pairing

To make the secure connection without holding the handheld device directly up to the base station, proceed as follows:

1) Press the Ident key on the handheld device for at least 3 s.
2) The "System State" dialog opens.

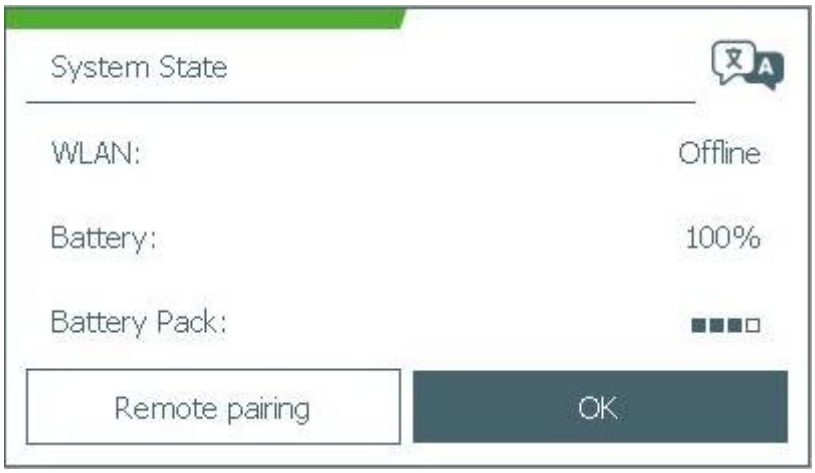


Fig. 11-97: "System State" dialog.

3) Tap "Remote pairing" and enter the password.
4) Enter the MAC address of the desired base station. Alternatively, you can select the name from the stored list of base stations.
5) Selection of the LED pattern shown on this desired base station at this time.

KEBA © KEBA 2021

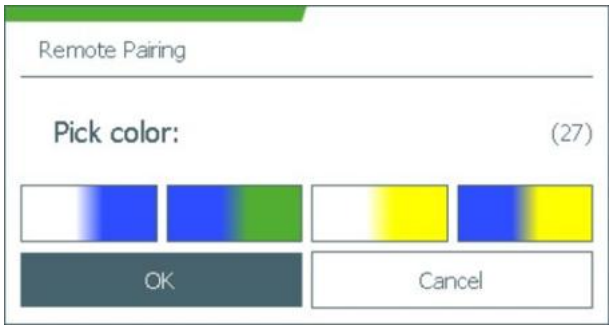


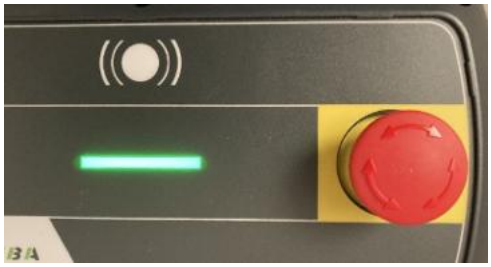
Fig. 11-98: LED pattern dialog

6) Confirm with "OK".

The secure connection is established. You can tell the connection has been established successfully by the illumination status of the LED bar of the base station and the emergency stop of the handheld device. This must be verified using a visual inspection.

Information

If remote pairing is performed outside the defined operation area, the operation area monitoring responds immediately with the infringement area measures. The emergency stop is triggered and the machine enters a safe state.

Base station connected	Handheld device connected
	

Depending on which configuration is set, the handheld device connects automatically to the base station or hall network for functional data exchange.

Remote Unpairing

To disconnect the secure connection without holding the handheld device directly up to the base station, proceed as follows:

1) Press the Ident key on the handheld device for at least 3 s.
2) The "System State" dialog opens.

© KEBA 2021

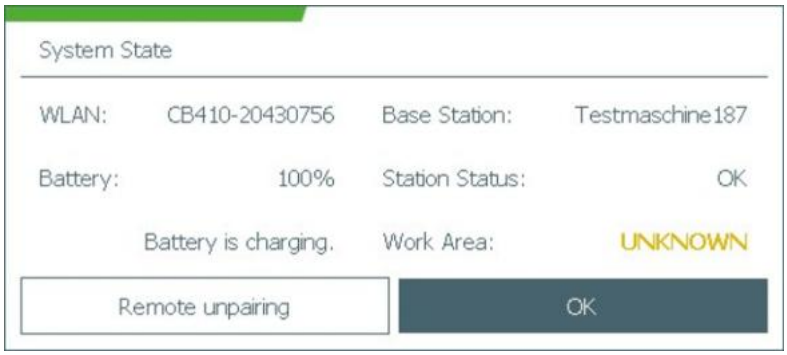


Fig. 11-99: "System State" dialog.

3) Tap "Remote unpairing" and enter the password.

4) Selection of the LED pattern shown on this desired base station at this time.

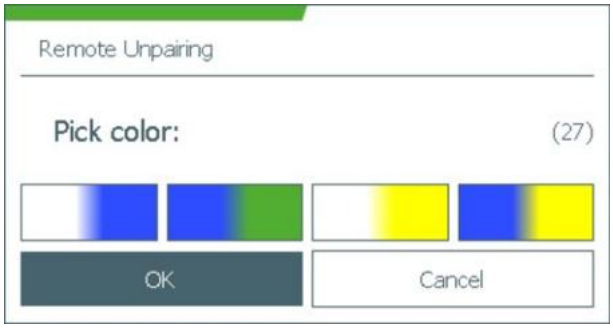
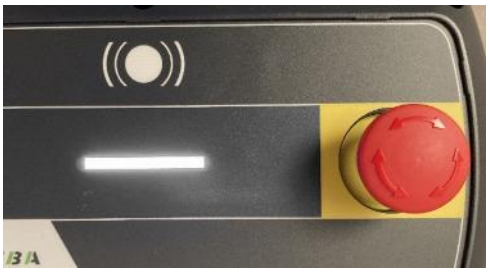


Fig. 11-100: LED pattern dialog

5) Confirm with "OK".

The secure connection is disconnected. You can tell the connection has been disconnected successfully by the illumination status of the LED bar of the base station and the emergency stop of the handheld device. This must be verified using a visual inspection.

Base station disconnected	Handheld device disconnected
	

Depending on which configuration is set, the handheld device connects automatically to the hall network for functional data exchange or remains offline.

KEBA © KEBA 2021

It is important that such a changeover from automatic to special operation mode is possible only once! The "Pairing/special pairing" outputs must not be used for the reset from special operation mode to automatic mode. Either a key-operated switch or another measure must be used.

© KEBA 2021

12 Diagnosis

This chapter describes the possible error states and how to rectify them.

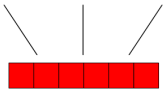
Information

When the optional operation area monitoring is used, an error can be acknowledged only within the operation area.

If an error occurs, it is indicated via the LED status bar on the base station.

Display	Error	Remedy
Blue	Serious error: LED of the illuminated emergency stop on the connected handheld device is faulty. An emergency stop is triggered.	The error can be acknowledged during live operation. Rectify this error by replacing the illuminated emergency stop button or connecting a handheld device for which the LED of the illuminated emergency stop button is functional.
Half red / half blue	OAM error: Error during operation area monitoring	Disconnect the connection to the device. Activate and unlock the emergency stop.
Yellow	Fieldbus error (only for CB42x and CB43x): No fieldbus communication occurs. The F-address is set incorrectly.	Check the F-address setting. Check the connection and setting of the fieldbus connection.
Flashing yellow	Fieldbus error: Restart of the base station or F-host. Communication error between base station and F-host. F-host requests the safe state of the base station.	User acknowledgment on the F-host required.
Flashing half yellow / half red	Serious error: The error indicated with blue LEDs was not rectified.	The error can be acknowledged during live operation. Connecting a handheld device with functional illuminated emergency stop.
Flashing half yellow / half red	Serious error: The emergency stop has been triggered. The base station was de-energized and the emergency stop unlocked. When the base station is restarted, an error is displayed and the emergency stop is triggered again.	The error can be acknowledged during live operation. Activate and unlock the emergency stop.

KEBA © KEBA 2021

Display	Error	Remedy
Flashing half yellow / half red	Serious error: The emergency stop circuits of a switching element are asynchronous. An emergency stop is triggered.	The error can be acknowledged during live operation. Activate and unlock the affected emergency stop.
Flashing half yellow / half red	Serious error: A broken connection was restored automatically. An emergency stop is triggered.	The error can be acknowledged during live operation. Activate and unlock the emergency stop.
Flashing red 	Fatal Error: A safety-critical hardware error has been detected. An emergency stop is triggered. Possible error when selecting the DIP switches for the OAM configuration or the gateway F-address.	The error cannot be acknowledged during live operation. The base station must be replaced. Please follow the procedure for setting the OAM limits (see 8.3 Operation area configuration (safety-related)) and for setting the gateway F-address (see 8.2 F addressing (only for CB42x and CB43x)).
Red chaser light	Disconnection: The connection to the handheld device was interrupted.	Restore the connection to the handheld device.
Red	Emergency stop actuated: Safe state was triggered.	Unlock the emergency stop (see 9.3 Base station operating states).

All errors triggered by the handheld device can be acknowledged after unpairing. Then the LED bar of the base station lights up white.

© KEBA 2021

13 Maintenance

The base station is maintenance-free. No repairs of any kind may be carried out.

The following activities can be carried out on the handheld device:

- Cleaning the touchscreen
- Changing the battery
- Creating a status report
- Creating a backup
- Restoring from a backup
- Replacing the SD card

13.1 Cleaning the touchscreen

Caution

Never clean the touchscreen with solvents, scouring agent or scrubbing sponges. Otherwise the touch surface could be damaged!

For cleaning the device, use a soft cloth and a bit of water or a mild cleaning agent. The cleaning agent should be sprayed onto the cloth and not directly onto the surface.

Via the symbol

on the desktop the Touch clean mode can be activated which deactivates the touch surface for a configured time (minimum 20 seconds). In this time the display can be cleaned without accidentally executing any actions on the touch surface.

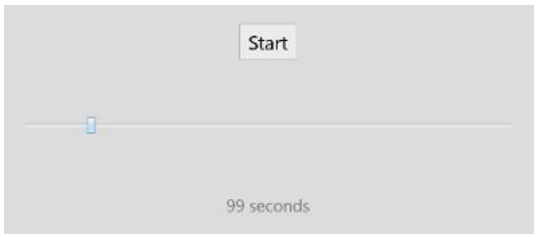


Fig. 13-101: Touch clean mode

After this time the desktop is displayed again.

13.2 Changing the battery

If the battery no longer supplies power despite being fully charged, it can be replaced. A new battery can be ordered from KEBA.

KEBA © KEBA 2021

Information

- The seal of the connection slot must be clean, undamaged and in the correct position.
- No cables must be trapped.

To replace, proceed as follows:

1) Switch off the power supply.
2) Remove the handheld device.
3) Unscrew the 4 screws using a screwdriver (see 4.6.2 Plugging in battery).
4) Remove the slot cover.
5) Disconnect the battery connection cable in the connection slot.
6) Connect the new battery connection cable in the connection slot.
7) Close the slot cover.
8) Tighten the slot cover using the screwdriver (torque: 0.8 bis 1.0 Nm).

The battery has been replaced.

Information

In order to comply with the information obligation, detailed information of the battery is provided in the product safety data sheet. The document can be downloaded from https://support.keba.com (under "Regulations").

13.3 Creating a service medium

A service medium with the Bootable Service System (BSS) program is required to create/restore a backup or to perform an update.

To create a service medium with an executable bootable service system (BSS), BSS can either be requested from KEBA support (e.g. as *.zip file) or created via KeStudio.

The following is required for creating a service medium:

- Empty USB drive with min. 32 GB free storage and formatted with FAT32.

Creating via archive file

To create a service medium via an archive file, the archive (e.g. *.zip file) provided by KEBA must be extracted and copied into the `\boot` directory of the root directory of the service medium. Subsequently, the file `prepare.cmd` must be executed inside the `\boot` directory.

© KEBA 2021

Creating via KeStudio

To create a service medium via KeStudio, see the online help.

13.4 Creating a backup

The following is required for the backup procedure:

- Service medium (USB stick) with at least 20 GB free storage space

For more information about creating a service medium, see 13.3 Creating a service medium.

Information

It is recommended to copy the backup files to a secure EDP system since the data security on a USB stick cannot be guaranteed over longer periods of time.

Performing backup

To perform the backup, the following is required in addition to the service medium:

- USB hub
- USB keyboard

To create a backup, proceed as follows:

1) Plug the USB hub into the KeTop.
2) Plug the service medium and keyboard into the USB hub.
3) Perform a restart (disconnect power supply and reconnect).
4) Enter the BIOS by pressing F7 when the splash screen appears during the boot process.
5) Enter the BIOS password 7090. It takes approx. 30 seconds until the BIOS boot menu is displayed.
6) Select the service medium and press Enter.
7) Select the "Backup & Restore" menu item displayed in the started BSS.
8) Select "Backup" from the displayed menu.
9) Select the target medium to save the backup on and confirm with "Backup."
10) Confirm and start the backup with the "OK" button. A progress bar is displayed. The process takes between 15 minutes and 1 hour, depending on the USB stick used.

KEBA © KEBA 2021

Information

The storage medium must never be pulled out during the writing process.

11) After a successful backup, confirm the dialog.

12) Unplug the USB hub.

13) Select "Shutdown" to shut down or "Reboot" to reboot the handheld controller in the displayed menu.

The backup was created and stored in the `\images` directory on the USB stick. For each backup, a directory is created with the device designation, date and time.

13.5 Restoring a backup / Performing an update

The following is required to restore a backup or perform a software / firmware update:

- Service medium (USB stick) with at least 20 GB free storage space
- Backup or update files

For more information about creating a service medium, see 13.3 Creating a service medium.

To restore a backup or to perform an update, create the `\images` directory in the root directory of the service medium. The backup or update files must be copied into this directory.

Information

A backup may only be restored to the device on which it was created. Cloning devices is not permitted.

Caution

The service medium must not be disconnected during a process. A permanent power supply must be ensured (e.g. fully charged battery, plugging the device into the charging station). Otherwise, the firmware on the components may be destroyed, making further operation impossible.

Restoring a backup / performing an update

The following is required for this process in addition to the service medium:

- USB hub
- USB keyboard

For this process, proceed as follows:

© KEBA 2021

1) Unpairing zwischen Handbediengerät und Basisstation durchführen (siehe 11 Verbinden mit Basisstation).
2) Plug the USB hub into the KeTop.
3) Plug the service mediums and keyboard into the USB hub.
4) Perform a restart (disconnect power supply and reconnect).
5) Enter the BIOS by pressing F7 when the splash screen appears during the boot process.
6) Enter the BIOS password 7090. It takes approx. 30 seconds until the BIOS boot menu is displayed.
7) Select the service medium and confirm with Enter.
8) Select the "Backup & Restore" menu item in the displayed BSS.
9) Select "Restore" from the displayed menu.
10) Select the desired service medium as the source for the restore or update and confirm with the "Restore" button.
11) Pressing "OK" in the confirmation dialog starts the restore/update process and a progress bar is displayed. The process takes around 15 - 20 minutes depending on the USB stick used.

Information

The service medium must never be pulled out during the write operation

12) Confirm the dialog after a successful restore procedure.
13) Unplug the usb hub
14) Select "Shutdown" to switch off or "Reboot" to restart the hand-held pendant station in the menu displayed.

The backup has been restored or the software / firmware has been updated.

13.6 Replacing the storage medium

To replace the storage medium on the handheld device, proceed as follows:

1) Turn off the power supply.
2) Open the connection slot.
3) Press lightly on the old memory card in the slot until you hear a click and remove the released memory card.
4) Insert the new memory card into the slot and apply light pressure until it engages (audible click); the card will spring back slightly and engage. Insert in the proper direction!
5) Close the connection slot.

The storage medium has been replaced.

KEBA © KEBA 2021

Proper handling of flash storage media

Improper insertion can cause damage to the contact pins.

Do **not use force** when inserting the storage media into the slot. It is constructed so that it can only be inserted in one direction and it should slide into the slot easily with little force.

The flash storage media:

- should be kept away from moisture, heat and direct sunlight,
- should be protected against static electricity,
- should not be dropped or bent,
- should not be removed or the device switched off while the card is being written to.

© KEBA 2021

14 Disposal

14.1 Disposal of the module

Caution

Please observe the regulations regarding disposal of electric appliances and electronic devices!

Electrical and electronic devices including their accessories must be disposed properly. The materials are recyclable in accordance with their labeling. You can make an important contribution to protecting our environment by reusing, renewing and recycling materials and old appliances.

The product must not be disposed of with household waste.

14.2 Disposal of the battery

The crossed-out wheeled bin symbol indicates that batteries must not be disposed of with household waste.

When disposing of batteries, national and local regulations for proper disposal must be observed. Although batteries have a low voltage, they can react to significant heat exposure and mechanical damage. However, careful handling and proper disposal can largely prevent uncontrolled and hazardous reactions. To prevent short circuits and the associated heat buildup, batteries must never be disposed of together with conductive materials. Before disposal, the contacts should be insulated with adhesive tape if possible.

KEBA © KEBA 2021

CAUTION!

Danger to persons due to fire hazard or chemical burn!

The battery must only be used for the intended use.

The battery must not be dismantled, opened or crushed.

The battery must not be short-circuited.

Charging station and cables must show no signs of damage.

In case of battery leakage, the fluid must not come into contact with the skin or eyes. In case of contact, wash the affected area with plenty of water and see a doctor.

Do not subject the battery to mechanical shock, crush, impact, or puncture.

The battery must not be exposed to fire or heat.

The battery must not be exposed to dirt or humidity.

The battery must not be disposed as residual waste but must be recycled according to national and local regulations. Before disposal, the battery must be completely discharged or the contacts must be isolated with adhesive tape.

The battery may only be replaced by a battery purchased from KEBA. Use of another battery may present a risk of fire or explosion.

Caution

Battery failure due to improper handling!

The battery must be charged before first use.

- Avoid direct exposure to sunlight.
- Store the battery in a cool, dry, and well-ventilated area.
- Store the battery in an environment free of dust and corrosive gases.
- Do not leave the battery in the charger for more than 24 hours.
- The battery must be charged completely before first use.
- The battery must only be stored in its original packaging. Avoid containers in which loose metallic parts could cause short circuits.
- Do not store the unpacked battery in containers in which loose metallic parts could cause short circuits.
- Do not store a battery longer than 1 month in a discharged state.

© KEBA 2021

15 Technical data

15.1 General

Protection class:	III according to EN 61131-2 resp. EN 50178
Protection type:	IP65

15.2 Environmental conditions

Operating temperature:	
• Handheld device:	0 °C to 40 °C.
• Base station:	0 °C to 50 °C
Storage and transport temperature:	-25 °C to +50 °C
• Handheld device with battery:	-25 °C bis +50 °C
• Handbediengerät without battery:	-25 °C bis +70 °C
• Base station:	-25 °C bis +70 °C
Relative air humidity (non-condensing):	5% to 95% (non-condensing)
Vibration resistance according to IEC 60068-2-6:	
• With 3.5 mm:	5 Hz ≤ f <8.4 Hz
• With 1 g:	8.4 Hz ≤ f < 150 Hz
Shock resistance according to EN 61131-2 or EN 60068-2-27:	15 g / 11 ms
Installation altitude:	Max. 2,000 m above sea level

15.3 Safety characteristics

Handheld device general information

Usage duration:	20 years
Emergency stop:	SIL 3, category 4, PL e
Enabling switch:	SIL 3, category 4, PL e

WARNING!

To ensure that the characteristic values are maintained, the handheld device must be decommissioned after 250.000 actuations of the integrated emergency stop switching element and/or 1,000.000 actuations of the integrated enabling switch switching element or no later than 20 years (service life).

T15xWL with emergency stop (type FRVKD_R0)

PFH_D value:	$1{,}05^{-09}$ 1/h

KEBA © KEBA 2021

$MTTF_D$[a] value:	356
DC_{avg} value:	98 %
Classification:	HIGH
$B10_D$ value:	250.000
n_{op} value (typical):	52

T15xWL with enabling switch (type HE6B)

PFH_D value:	$1{,}53^{-09}$ 1/h
$MTTF_D$[a] value:	310
DC_{avg} value:	98 %
Classification:	HIGH
$B10_D$ value:	2.000.000
n_{op} value (typical):	8.760

T15xWL with enabling switch (panic contact, type HE6B)

PFH_D value:	$1{,}03^{-09}$ 1/h
$MTTF_D$[a] value:	358
DC_{avg} value:	98 %
Classification:	HIGH
$B10_D$ value:	1.000.000
n_{op} value (typical):	52

Base station general information

Usage duration:	20 years
Emergency stop:	SIL 3, category 4, PL e
System response time for emergency stop:	19 ms

WARNING!

To ensure that the characteristic values are maintained, the base station must be decommissioned after 250.000 actuations of the integrated emergency stop switching element or no later than 20 years (service life).

CB41x / CB42x / CB43x with emergency stop (type FRVKOO)

PFH_D value:	$1{,}11^{-09}$ 1/h
$MTTF_D$[a] value:	254
DC_{avg} value:	98 %
Classification:	HIGH
$B10_D$ value:	100.000
n_{op} value (typical):	52

System

Usage duration:	20 years

© KEBA 2021

Emergency stop:	SIL 3, category 4, PL e
Enabling switch:	SIL 3, category 4, PL e
System response time (WCDT)*):	430 ms

*) The system response time is the time between actuation of the emergency stop switch or the enabling switch and switching of the base station outputs (worst case scenario). The value of the system response time has been determined empirically by KEBA and ensures a stable system in a conventional industrial radio environment. Typical response times of the system are in the 40 - 80 ms range. If, as part of a general safety consideration, it becomes necessary to adapt the system response time, contact KEBA.

CB42x PROFIsafe characteristics

DAT (Device Acknowledge Time):	61 ms

MTTF calculation

For the calculation of the overall safety function, the specified total PFH_D of the safety electronics is to be used. The illuminated emergency stop on the handheld device and the emergency stop on the base station must also be considered. This is based on the specified B_{10D} value. From this, the $MTTF_D$ value must be calculated as follows:

$$MTTF_D = \frac{B_{10D}}{0{,}1 * n_{op}} \qquad n_{op} = \frac{d_{op} * h_{op} * 3600}{t_{Cycle}} \qquad MTTF_D = \frac{B_{10D} * t_{Cycle}}{360 * d_{op} * h_{op}}$$

For details on the abbreviations, see chapter 1.7.3 Abbreviations. The $MTTF_D$ value can now be transferred to a PFH_D (x = number of hours per year):

$$MTTF_D = \frac{1}{x * PFH_D} = \frac{1}{8760 * PFH_D}$$

Then, the PFH_D values must be added to the overall safety function in acc. with EN ISO 13849-1

$PFH_D = PFH_{D\ electronics} + PFH_{D2\ switching\ element} + \ldots + PFH_{DN}$

15.3.1 System response time with safe fieldbus connection (for CB42x and CB43x)

To calculate the response time of the safety function, you must assume the maximum delay time of the wireless system in case of an error (WCDT). In addition, the watchdog time of the safe fieldbus and the cycle time of the F-host must be taken into account.

KEBA © KEBA 2021

Information

In this manual, only the response time of the safety function between the wireless system and the F-host is specified. Potential further safety modules (e.g. safe digital output modules) are not considered here.

The following formula is available for the calculation:

OFDT	Worst-case delay time in case of an error (one fault delay time)
WCDT	Worst-case delay time (For system response time, see 15.3 Safety characteristics)
WDTime	Watchdog time of the safe fieldbus connection
$Tcy_{F\text{-}Host}$	F-Host cycle time

$OFDT = WCDT + WDTime + Tcy_{F\text{-}Host}$

15.4 Mechanical properties

Handheld terminal

Construction:	PPE/PS housing
Flame retardance:	UL94-V0
Safe drop height (2 falls according to EN 61131-2):	1 m (on industrial floor), then at least protection class IP54

Base station

Construction:	ABS-PC housing

15.5 Battery / Rechargeable Battery

Battery – Panasonic BR2032

Manufacturer name:	Panasonic
Battery category:	Device battery
Model designation:	BR2032
Chemical designation:	Lithium polycarbon monofluoride battery
Battery weight:	8 g
Nominal voltage:	3 V
Capacity:	1000 mAh
Rechargeable:	No
Replaceable:	No

Rechargeable Battery - Celltech 169-2001

Manufacturer name:	Celltech
Battery category:	Device battery
Model designation:	169-2001

© KEBA 2021

Chemical designation:	LI-IO
Battery weight:	100 g
Nominal voltage:	7.2 V
Capacity:	3450 mAh
Rechargeable:	Yes
Replaceable:	Yes

15.6 Technical data handheld device

15.6.1 General

Display:	10,1" TFT (16:10) LED backlight 1.280 x 800 pixels (WXGA)
Touchscreen:	Projective capacitive
Keyboard:	Membrane keypad with tactile feedback Maximum 30 buttons 6 status LEDs

15.6.2 Power supply

Handheld device

Charging voltage:	24 V DC (rated voltage tolerance range 19.2 V DC to 29 V DC SELV/PELV in accordance with EN 61010-2-201)
Power consumption:	Up to 43 W (1.8 A at 24 V DC)
Connection option:	Supply via charging contacts or DC socket

Battery

Battery chemicals:	Lithium ion
Nominal voltage:	7.2 V
Nominal capacitance:	3.5 Ah
Energy content:	25.2 Wh
Charging option:	Integrated into handheld device via the device power supply
Typical operating time:	Approx. 1.5 h
Typical charging time to 80 % capacity:	Approx. 1.2 h

15.6.3 Processor

Processor:	
• 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

KEBA © KEBA 2021

• KeTop Txx-xxx-x**N**x-xxx, KeTop Txx-xxx-x**f**x-xxx	Celeron N2807 Dual Core 1,58 GHz
Memory RAM:	
• Atom x6211:	4 GB (DDR4x) 8 GB (DDR4x)
• Celeron N2807:	4 GB (DDR3L)
Memory FLASH (Celeron N2807 only):	8 GB eMMC
Memory SSD (extended memory):	64 GB SSD
Operating system:	Windows 10 IoT Enterprise 2016 LTSB or Windows 10 IoT Enterprise 2021 LTSC

15.6.4 Interfaces

Wireless interface

Number:	3
WLAN:	WIFI 802.11 a b g n ac
• Frequency bands:	2,400 - 2,483.5 MHz / 5150 - 5,350 MHz / 5,470 - 5,725 MHz
• Transmitting power:	Max. < 10 dBm
• Encryption:	WPA2-PSK with CCMP
Bluetooth:	BT 4.2 BLE
• Frequency bands:	2,400 - 2,483.5 MHz
• Transmitting power:	Max. < 10 dBm
Operation area monitoring:	
• Frequency bands:	2,400 - 2,483.5 MHz
• Transmitting power:	Max. < -1.21 dBm

USB interface

Quantity:	1
Type:	USB 2.0 (Hi-Speed)
Output current:	Max. 500 mA

RFID interface (for connection to base station)

Number:	1
Range:	Min. 2 cm
Transponder chip:	I-Code SLI (according to ISO 15693)
Frequency bands:	13.553 - 13.567 MHz
Transmitting power:	Max. < 0,15 A/m

Micro SD interface

Quantity:	1

© KEBA 2021

15.6.5 Dimensions, weight

KeTop T150WL

Height (including emergency stop):	284 mm
Width:	215 mm
Depth:	
● Without handle:	69 mm
● With handle:	76 mm
Weight:	Approx. 1,450 g

KeTop T155WL

Height (including emergency stop):	215 mm
Width:	284 mm
Depth:	
● Without handle:	69 mm
● With handle:	76 mm
Weight:	Approx. 1,450 g

15.7 Technical data base station

15.7.1 Power supply

Power supply:	24 V DC (rated voltage tolerance range 16 V DC to 30 V DC SELV/PELV in accordance with EN 61010-2-201)
Inrush current:	9 A (for approx. 2 ms)
Power consumption:	14.4 W (600 mA at 24 V DC)
Max. interruption time of the supply voltage:	≤ 10 ms (according to EN 61131-2)

15.7.2 Interfaces

Wireless interface

Number:	3
WLAN:	WIFI 802.11 a b g n ac
● Frequency bands:	2,400 - 2,483.5 MHz / 5150 - 5,350 MHz / 5,470 - 5,725 MHz
● Transmitting power:	Max. < 10 dBm
● Encryption:	WPA2-PSK with CCMP
Bluetooth:	BT 4.2 BLE
● Frequency bands:	2,400 - 2,483.5 MHz
● Transmitting power:	Max. < 10 dBm
Operation area monitoring:	
● Frequency bands:	2,400 - 2,483.5 MHz

KEBA © KEBA 2021

• Transmitting power:	Max. < -1.21 dBm

Ethernet interface

Number:	2
Data transmission rate:	100 Mbps

EtherCAT interface

Number:	2
Data transmission rate:	100 Mbit/s

PROFINET interface

Number:	2
Data transmission rate:	100 Mbit/s

"Pairing" / "Remote Pairing" outputs

Number:	2
Nominal voltage (Ue):	24 V DC
Current carrying capacity:	Max. 100 mA
Specified polarity:	No
Isolation:	500 V AC (1 min) to the rest
Output testing:	No

15.7.3 Terminal strips

General data

Connection type:	Push-in spring connection
Plug-in:	Yes
Conductor cross-section rigid/flexible:	0.2 - 1.5 mm²
Conductor cross-section AWG / kcmil:	16 - 24
Conductor cross-section, flexible with wire end sleeve without plastic sleeve:	0.25 - 1.5 mm²
Conductor cross-section, flexible with wire end sleeve with plastic sleeve:	0.25 - 0.75 mm²
Stripping length:	10 mm
System response time FRB (typical):	40 ms

Terminal strip S1

Number:	1
Model:	CB41x:11-pole CB42x: 2-pole CB43x: 2-pole
Nominal voltage (Ue):	24 V DC
Specified polarity:	Yes
Isolation:	Yes

© KEBA 2021

Output testing:	No

Terminal strip S2

Number:	1
Nominal voltage (Ue):	24 V DC
Current carrying capacity:	Max. 700 mA
Current requirement:	Min. 1 mA
Specified polarity:	No
Isolation:	Yes
Output testing:	No

Signal terminal strip

Number:	1
Nominal voltage (Ua at 24 V pin):	24 V DC
Current carrying capacity:	Max. 100 mA per output (signal color at the column) or 500 mA at 24 V pin
Specified polarity:	Yes
Isolation:	No
Output testing:	No
Output type:	Open Collector output to GND

Terminal strip for "Fast Response" buttons

Number:	14
Nominal voltage (Ua):	Switched 24 V DC to GND on the same terminal strip
Current carrying capacity:	Max. 20 mA per output
Specified polarity:	Yes
Isolation:	No
Output testing:	No

15.7.4 Enabling function

Function

Output type:	Safe semiconductor outputs
Switching element:	Two-circuit electromechanical
Nominal voltage (Ue):	24 V DC
Rated current (Ie):	Max. 250 mA (per circuit)
Short circuit and overload protection:	No
Isolation:	500 V AC (1 min) to the rest
Usage category:	DC13 (in acc. with IEC 60947-5-1)
Reverse voltage protection:	Yes
Output testing:	Yes (test pulse duration <=2 ms)
Grip change function:	Yes

KEBA © KEBA 2021

Output synchronization:	Yes

Switching element

Switching element:	Two-circuit electromechanical
Operating forces:	
● From switch position 1 to 2:	3 N typical
● From switch position 2 to 3:	17 N typical
B_{10D} value (1-2-3-1):	1.000.000

15.7.5 Emergency stop function

Function

Output type:	Safe relay outputs
Switching element:	Two-circuit electromechanical
Nominal voltage (Ue):	24 V DC
Minimum current (Ie):	10 mA (per contact)
Maximum current carrying capacity:	1,000 mA (per contact)
Usage category:	DC-13 (in acc. with IEC 60947-5-1)
Output synchronization:	Yes
Isolation:	500 V AC (1 min) to the rest

Switching element

Switching element:	Two-circuit electromechanical, rotary unlocking
B_{10D} value.	250,000

Illuminated emergency stop

Illumination type:	LED lighting
Luminosity:	Type 11700 mcd
Service life:	Service life 80,000 - 100,000 h

15.7.6 Dimensions, weight

CB41x

Height:	162 mm
Width:	221 mm
Depth:	70 mm (without emergency stop)
Weight:	Approx. 760 g

CB42x

Height:	167 mm
Width:	223 mm
Depth:	95 mm (without emergency stop)

© KEBA 2021

Weight:	Approx. 600 g

CB43x

Height:	167 mm
Width:	223 mm
Depth:	95 mm (without emergency stop)
Weight:	Approx. 600 g

KEBA © KEBA 2021

16 Optional operating elements

This chapter describes the various options that are available with the devices. The optional elements are limited by the installation space and thus can be mutually exclusive.

16.1 Rotary Encoder Switch with 16 positions

The T15xWL can be equipped with a rotary switch (16 positions, 4 bit Gray code), which is evaluated by default using software (via HWAPI or connection protocol).

16.2 Key-operated switch

The T15xWL and the base station can be equipped with a key-operated switch.

On the handheld device, the key-operated switch can be evaluated using software (via HWAPI or connection protocol). On the base station, the key-operated switch is directly wired and cannot be evaluated using the software. The key -operated switch is not evaluated by the safety electronics and is therefore not part of the type examination.

WARNING!

When evaluated by software there can be incorrect state evaluations in case of a software error. If the position of the key switch is safety-related this electromechanical switching element must be wired directly (without electronical evaluation on the KeTop) into the safety logic.

Caution

The safety logic must check the position of the key witch on exclusivity to simulaneously detect multiple selected modes.

The key-operated switch is available with 2 or 3 positions.

Depending on the variant of the equipped key-operated switch, it has one or more pull-out positions.

16.3 Illuminated push button

The T15xWL and the base station can be equipped with an illuminated push-button.

On the handheld device, the illuminated pushbutton can be evaluated and controlled using software (via HWAPI or connection protocol). On the base station, the illuminated pushbutton is directly wired and cannot be evaluated using the software.

© KEBA 2021

The illuminated pushbutton is available with a pulse or latching function.

WARNING!

When evaluating a switching element using the software, an error can cause an incorrect evaluation of the switching state. If the switching element is used for safety-oriented purposes, then this electromechanical switching element must be wired to the safety logic directly (without electronic evaluation on the KeTop level).

16.4 Handwheel

The T15xWL can be equipped with a handwheel. The handwheel pulses are evaluated in the processor and can be read out using software (via HWAPI or connection protocol).

50 pulses are counted per revolution. Rotating the handwheel clockwise increments the counter, while rotating it counterclockwise decrements the counter 0 to 65.535 (16-bit value).

Essential features:

- 50 notches/revolution
- 1 pulse/notch

Information

If the KeTop is dropped on the ground, check the mechanical fit of the adjusting knob. If necessary, the adjusting knob can be latched into place again by pressing it on from above.

16.5 Digital joystick

The handheld terminal can be equipped with a digital joystick. The digital joystick can be read out using software (via HWApi or connection protocol) on the handheld terminal. On the base station, the joystick is wired directly and can therefore not be evaluated via the software.

The digital joystick can be moved along 2 axes in 4 directions. The deflection of the joystick is detected with electrical normally open contacts and processed by logical operations of the 4 bits.

Key features:

- 2 directions / axis
- 1 Bit / deflection

KEBA © KEBA 2021

16.6 Camera

The T15xWL can be equipped with a camera on the rear.

Technical data

Video formats:	YUY2 / MJPEG
USB:	2.0
Image resolution:	5 megapixels 320 x 240 (min) / 640 x 480 (standard) / 2592 x 1944 (max)

© KEBA 2021

17 Accessories

17.1 KeTop CS 15x charging station

The charging station serves as a wall bracket and for charging the device and can be ordered under the following number:

Order number	Device
111903	KeTop CS15x

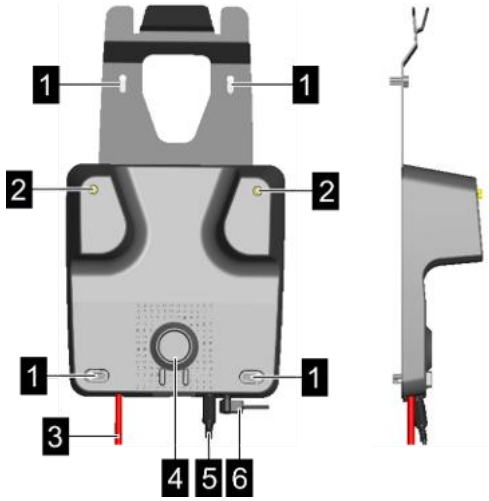


Fig. 17-102: Charging station

1 ... Drill hole	2 ... Charging contact
3 ... 24 V power supply cable via power adapter of the external power supply	4 ... Magnet pad for the battery pack
5 ... 24 V power supply for the battery pack (plug)	6 ... 24 V power supply via direct connection (plug)

Voltage supply via power adapter

The charging station can be supplied with voltage using a commercially available power adapter. For this purpose, on the charging station there is a DC socket 5.5/2.1 suitable for a DC barrel connector 5.5/2.1.

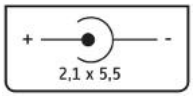


Fig. 17-103: Socket symbol

Power supply via direct connection

The charging station can be supplied with voltage using direct wiring. To do so, the charging station must be opened.

KEBA © KEBA 2021

Fig. 17-104: Connectors

1 ... 24 V (plus)	2 ... GND (minus)

Information

Operation of the charging station is only permissible with a correctly closed housing.

WARNING!

Risk of electric shock to persons!

- Supply the charging station exclusively from voltage sources which have protective extra-low voltage (e.g. SELV or PELV according to EN 61010-2-201).
- Connecting a SELV voltage source can, depending on the variant, turn it into a PELV voltage source.
- Only connect voltages and electric circuits that have a safe disconnect for hazardous voltages (e.g. with sufficient isolation and electric strength) to connections, terminals and interfaces with a rated voltage of up to 50 V.

CAUTION!

Fire hazard in the event of component failure!

Provide suitable fuses for the 24 V DC power supply of charging station supplying the device with power. For this purpose, a UL 248 approved fuse must be used at max. 3.15 A.

Only charge the handheld operating device with the chargers recommended by KEBA and with the intended charging means (charging station and power supply unit).

17.2 Power supply unit

The power supply unit is used to charge the device. It can be connected directly to the handheld control unit or to the charging station and can be ordered under the following number:

© KEBA 2021

Information

This power supply unit is an optional accessory intended exclusively for commissioning the wireless handheld terminal in office or laboratory environments.

Order number	Designation
128939	KeTop 24VDC supply set

Information

The power supply unit is not suitable for industrial environment and may therefore only be used in the living area (e.g. office). Since the KeTop may cause radio interference in living areas, charge only when switched off.

17.3 Battery

The handheld device must be operated with this battery or the battery pack only. The battery can be charged at the charging station and can be re-ordered under the following number:

Order number	Device
120048	KeTop T150WL Battery V1 (only Celeron N2807)
120049	KeTop T155WL Battery V1 (only Celeron N2807)
140626	KeTop T150WL Battery V2 (only Atom x6211)
140627	KeTop T155WL Battery V2 (only Atom x6211)
140915	KeTop T150WL Battery V2 (only Celeron N2807)
140916	KeTop T155WL Battery V2 (only Celeron N2807)

Also see about this

Configure hibernation [› 159]

KEBA © KEBA 2021

17.3.1 Battery Celeron N2807

Type plate

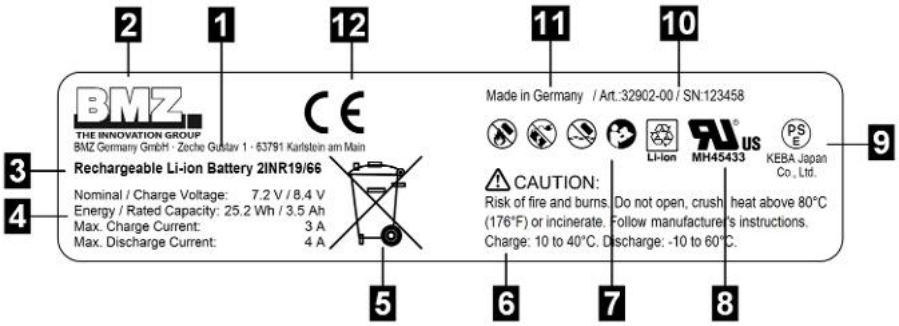


Fig. 17-105: Type plate

1 ... Manufacturer's address	2 ... Manufacturer
3 ... Product designation	4 ... Technical data
5 ... Advice on Waste Electrical and Electronic Equipment	6 ... Warning
7 ... Warning Symbols	8 ... UR marking
9 ... PSE marking	10 ... Material / serial number
11 ... Country of manufacture	12 ... CE marking of conformity

Battery life

The battery life depends on the configuration of the handheld terminal (see 8.7 Configure hibernation).

Information

If the battery capacity drops to 25 %, a warning is issued. From ≤15 %, the handheld terminal goes into the idle state.

Storage and transport

In the delivery state, the battery is unplugged and charged to 30 %. This corresponds to the optimal storage and transport condition. To maintain this state, the battery must be connected to the handheld terminal every 3 months, charged to 30 % and disconnected again.

The rechargeable battery must be fully charged before starting up the handheld operating device.

17.3.1.1 Technical data

Environmental conditions

Operating temperature:	0 °C to 40 °C
Storage and transport temperature:	-25 °C to +50 °C (ideal: 20 °C)

© KEBA 2021

Charging temperature:	10 °C to 40 °C
Relative humidity (non-condensing):	5 % to 95 % (ideal: 40 °C)
Operating altitude:	Max. 2000 m above sea level

17.3.2 Rechargeable Battery Atom x6211

Type plate

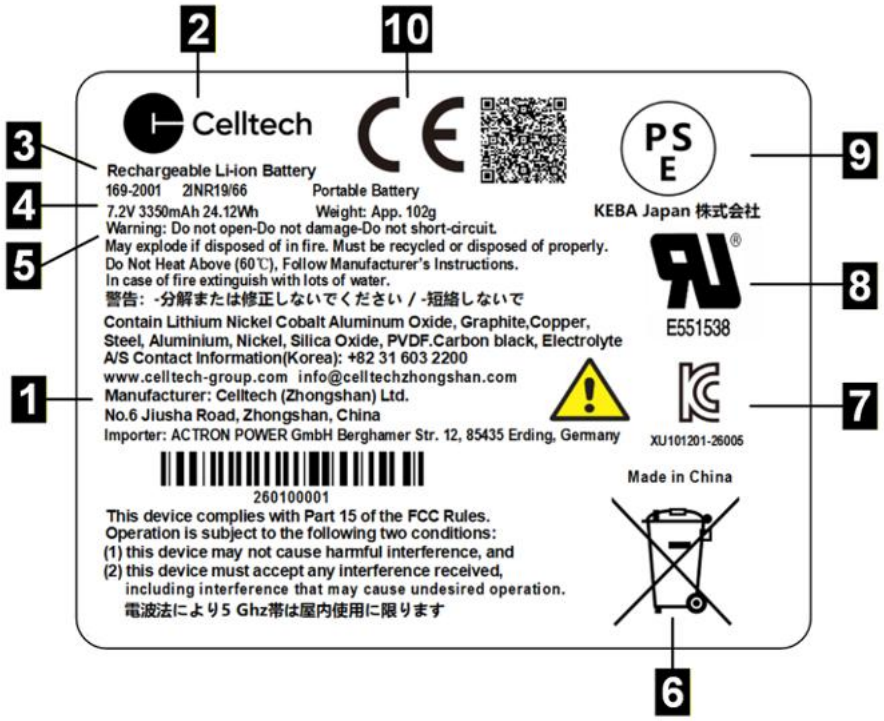


Fig. 17-106: Type plate

1 ... Manufacturer's address	2 ... Manufacturer
3 ... Product designation	4 ... Technical data
5 ... Warning	6 ... Disposal information
7 ... KC marking	8 ... UR marking
9 ... PSE marking	10 ... CE marking of conformity

Battery life

The battery life depends on the configuration of the handheld device (see 8.7 Configure hibernation).

Information

If the battery capacity drops to 25 %, a warning is issued. From ≤15 %, the handheld device goes into hibernation mode.

KEBA © KEBA 2021

Storage and transport

Upon delivery, the battery is disconnected and charged to 30 %. This corresponds to the optimal storage and transport condition. To maintain this state, the battery must be connected to the handheld device every 3 months, charged to 30 %, and then disconnected again.

Before starting up the handheld device, the battery must be fully charged.

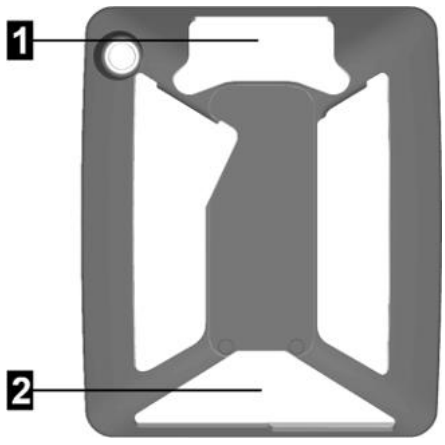
17.3.2.1 Technical data

Environmental conditions

Operating temperature:	-40 °C – 60 °C (discharging)
Storage and transport temperature:	-10 °C – 26 °C (1 year)
Charging temperature:	0 – 60 °C
Relative humidity (non-condensing):	35 – 85 % (relative humidity)
Operating altitude:	Max. 2000 m

17.4 Bumper / carrying set

The bumper serves as additional protection for the device against shocks or impacts and is available in the following variants:

Bumper vertical format	Bumper horizontal format
	

1	Handle recess	2	Cable recess

The bumper can be requested and purchased from KEBA.

Designation	Order number
Bumper vertical format (KeTop T150x)	125248
Bumper horizontal format (KeTop T155x)	122868

© KEBA 2021

Carrying set

The carrying set consists of the bumper and a carrying strap. The carrying set provides ergonomic relief and increased freedom of movement. It also increases safety and efficiency when handling the device.

WARNING!

Danger of personal injury due to strangulation or falling!

Improper use of the carrying set as a hoist for persons can lead to life-threatening injuries or death. Moving parts in the carrying set can lead to entanglement and strangulation.

- Never use the carrying set to lift or secure people.
- When handling the harness, watch out for moving parts and keep them away from body parts.

WARNING!

Danger of personal injury due to incorrect physical strain!

One-sided strain caused by additional attached accessories can lead to back pain and other muscle and joint injuries. Attaching unauthorized additional parts to the carrying set can impair safety and cause injuries.

- Avoid one-sided loading when using accessories such as the battery pack.
- Do not attach any other additional parts to the carrying set that are not expressly permitted.

WARNING!

Danger of personal injury due to hot surface or fire hazard!

Heated charging points can cause burns or trigger a fire in the carrying set if the charging contacts are not connected correctly.

- Ensure that the charging contacts of the charging station are not covered by a strap of the carrying set.
- The charging contacts of the hand-held device and the charging station must be in full contact to prevent overheating and the risk of fire.

KEBA © KEBA 2021

CAUTION!

Risk of tripping and obstruction of traffic routes!

Improperly placed or positioned devices and carrying sets can lead to tripping accidents and obstructions, which can cause minor to moderate injuries.

- Only attach the device including carrying set to the wall bracket or charging station.
- When not in use, store the carrying set safely away from traffic and danger areas.

The carrying set can be requested and purchased from KEBA.

Bezeichnung	Bestellnummer
Carrying set with bumper vertical format (KeTop T150)	136171
Carrying set with bumper horizontal format (KeTop T155)	136160

17.4.1 Attaching the bumper

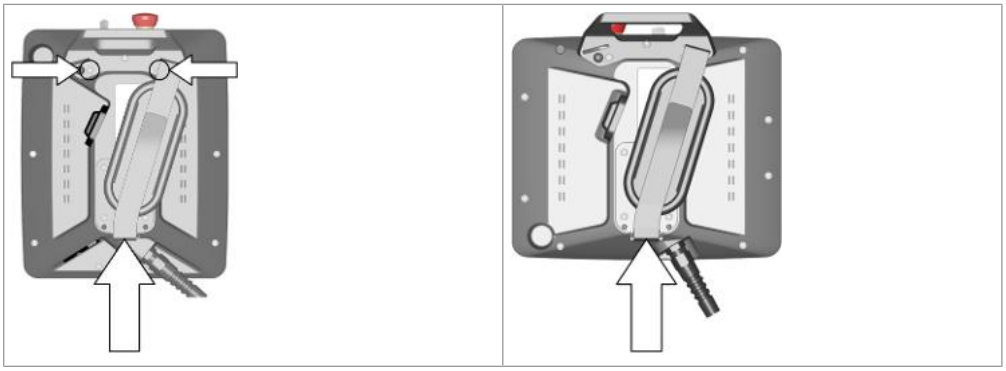
Caution

Improper handling can cause damage to the operating panel.

- Switch off the power supply before carrying out assembly, installation or maintenance work and unplug possible interface cables.
- Make sure that the work surface is clean, level and stable. The surface should be free of dust and foreign matter.
- Use a pad to protect the glass front from being scratched.

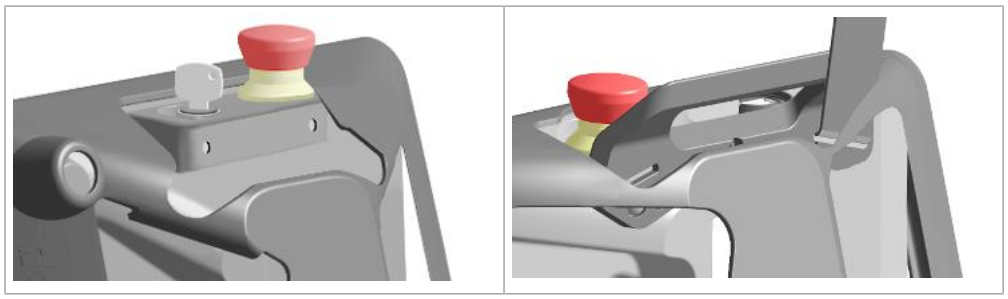
To attach the bumper, proceed as follows:

1) Switch off the handheld device.
2) If available: Unplug the connection cable.
3) Loosen the hand strap at the lower end and remove the handle (Torx10).



© KEBA 2021

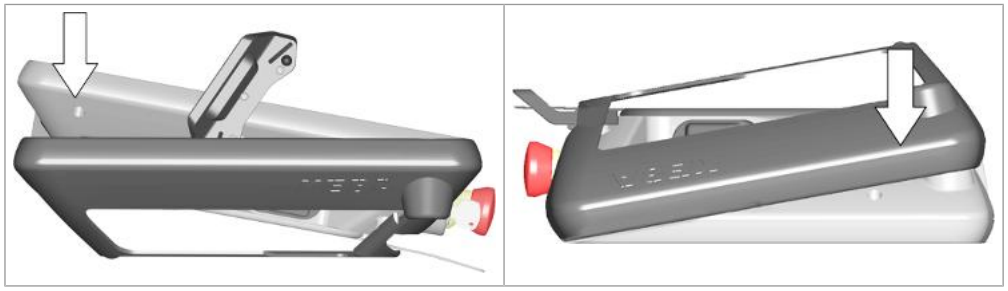
4) Hang the bumper on the emergency stop switch through the handle recess.



5) If available: Pull the connection cable through the cable recess of the bumper.

6) Clip the bumper over the upper edges.

7) Clip the bumper over the lower edges. The removed handle can be used as a mounting aid.



8) Mount the handle and the hand strap on the device.

The bumper is now completely mounted.

17.4.2 Cleaning

Caution

Damage to property due to improper cleaning or drying!

Improper cleaning or drying can damage the carrying set.

Only clean and dry the bumper and carrying strap in accordance with the instructions given here.

To clean the bumper and carrying strap, proceed as follows:

1) Remove the hand-held device from the bumper.

2) Clean the bumper with a soft brush (dry or damp). Make sure that no labels are damaged or rendered illegible.

3) Cleaning the carrying strap by hand: Clean the straps and ropes with lukewarm water or mild lukewarm soapy water (max. 40 °C). Do not use chemicals.

4) Rinse with clear lukewarm water.

KEBA © KEBA 2021

5) Leave to dry in an airy, dry and shady place. Do not expose the bumper and carrying strap to unnecessary UV radiation.

17.4.3 Storage and transportation

Caution

Damage to property due to improper storage or improper transportation!

Improper storage or transportation can damage the carrying set.

Only store and transport the bumper and carrying set in accordance with the instructions given here.

Always protect the bumper and carrying set from UV radiation and heat and ensure adequate ventilation during storage and transportation. Avoid airtight containers. It is recommended to use a UV-resistant material bag.

17.5 Handle and hand strap

A handle, with or without hand strap, can be mounted on the T15xWL. The handle is attached with 3 Torx screws (size 10). The hand strap can only be used when the handle is mounted.

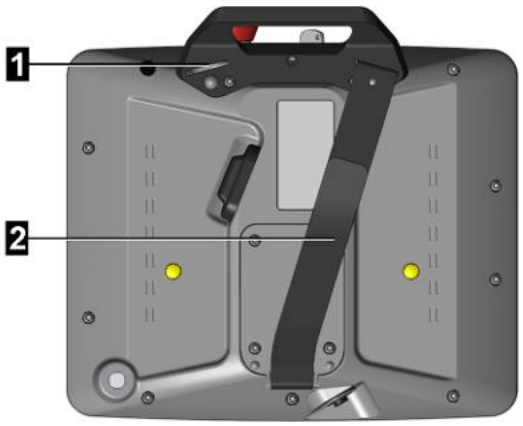


Fig. 17-107: T15xWL with handle and hand strap

1 ... Handle	2 ... Hand strap

17.5.1 Assembly

This chapter describes the assembly of the handle and hand strap. The following set is required for this:

Designation	Description	Order no.
Handle and hand strap T15x	Assembly set for handle and hand strap for KeTop T150 and KeTop T155	106420

© KEBA 2021

Caution

- Incorrect handling can result in damage to the handheld device. Switch the power supply off before performing mounting, installation and maintenance work.
- Make sure that the mounting surface is clean, level and stable. The surface should be free of dust and foreign matter.
- Use a pad to protect the glass front from being scratched.
- Only qualified, specialist personnel may perform the installation and commissioning of the product.

The following tool is required:

- Torx screwdriver size 10

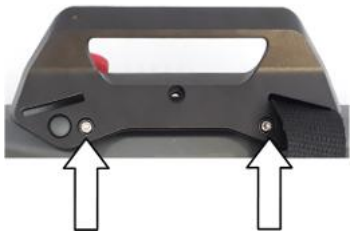
In order to mount the handle and hand strap, proceed as follows:

1) Switch off the power supply.
2) Remove the handheld device.
3) Store the handheld controller on the mounting surface with the touchscreen facing down.
4) Insert the thin end of the hand strap (1) through the desired slot on the handle (2). When doing so, the hook and loop fastener must be facing upwards.

5) Pull through the entire hand loop from back to front up to the wide end.
6) Attach the padding (optional). When doing so, the hook and loop fastener must be facing upwards (1).

7) Tighten the handle using the screwdriver (torque: 0.8 - 1.0 Nm) on the upper end of the handheld device.

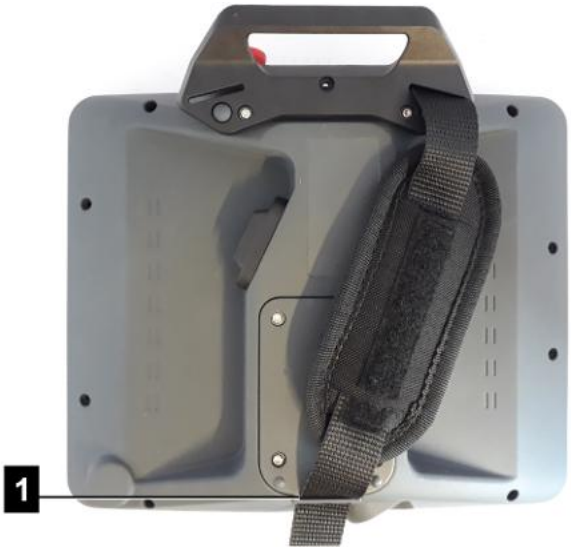
KEBA © KEBA 2021



8) Insert the hand strap through the slot on the lower end of the handheld device (1).

Information

Do not twist the hand strap when threading it through.



9) Pull the entire hand strap through.

10) Fasten the hook and loop fasteners together.

The handle and hand strap are now completely mounted and can be used.

17.6 Battery pack

The battery pack is used to extend the runtime of the handheld device. The battery pack must only be used for the handheld device. The battery pack can be charged at the charging station.

© KEBA 2021

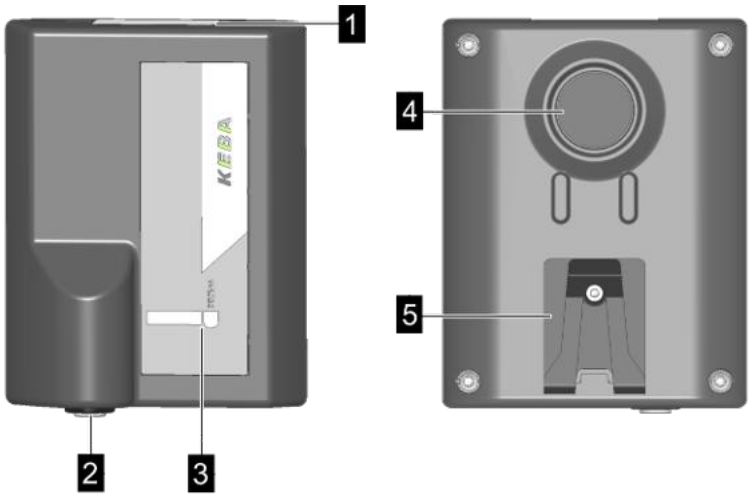


Fig. 17-108: Battery pack

1 ... Type plate	2 ... Socket for 24 V power supply of the charging station
3 ... Charge indicator with button	4 ... Magnet pad to attach to charging station
5 ... Belt clip (optional)	

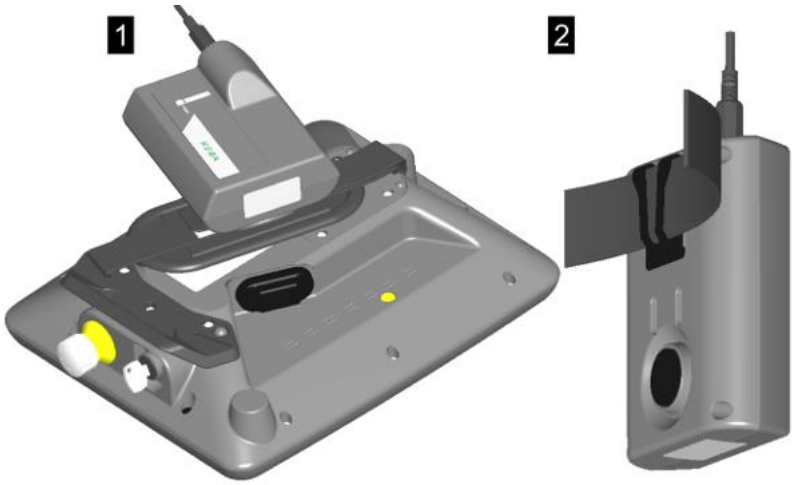


Fig. 17-109: Attachment of the battery pack

1 ... On the hand strap of the handheld device	2 ... On a belt

The battery pack is connected to the handheld device and can be attached to the hand strap of the device or to a belt using the belt clip. The belt clip is attached to the battery pack using the enclosed screw (Torx 8 screw head). Tighten the screw using 0.55 Nm torque.

The battery pack and its optional accessories can be ordered under the following numbers:

KEBA © KEBA 2021

Order number	Designation	Scope of delivery
131539	KeTop BP15xWL Set	• Battery • Box • Cable (short) • Hand strap clip
133130	Device mount KeTop BP15xWL	• Cable (short) • Hand strap clip
133131	Belt mount for KeTop BP15xWL	• Cable (long) • Belt clip
133179	KeTop BP15xWL	• Battery (no accessories)

Type plate

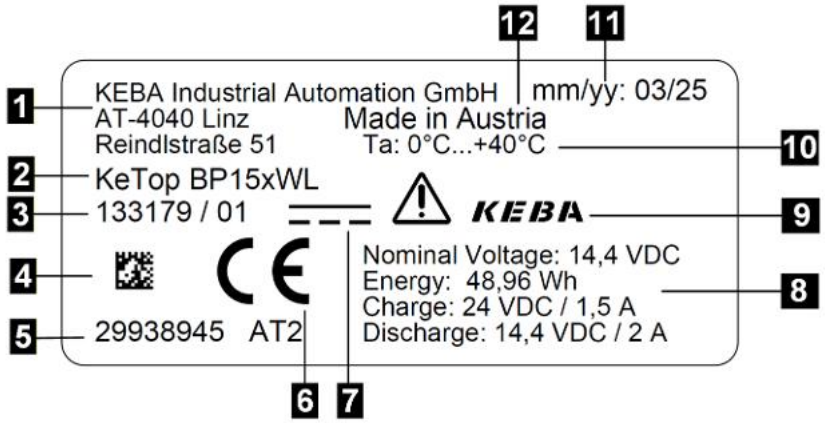


Fig. 17-110: Typen plate

1 ... Manufacturer's address	2 ... Product designation
3 ... Material / revision number	4 ... Data matrix code
5 ... Serial number	6 ... CE marking of conformity
7 ... Marking for separate disposal	8 ... Technical data
9 ... Manufacturer	10 ... Ambient temperature
11 ... Production date	12 ... Country of manufacture

Battery run time

Press the "PRESS" button to display the charge state on the charge indicator. Four LEDs display the current charge:

LED pattern	Charge
1 LED blinks	< 10%
1 LED lit	10 % - 25%
2 LEDs lit	26 % - 50%
3 LEDs lit	51 % - 75%
4 LEDs lit	76 % - 100%

© KEBA 2021

The service life of the battery pack depends on the ambient conditions and the type of usage. Usually, up to 800 charging cycles are possible, before the capacity begins to drop.

Storage and transportation

The battery pack is delivered with transportation mode on. With transportation mode on, the battery pack can be stored for longer periods without any drop in capacity.

Information

When transportation mode is on, the charging indicator is not functional.

The transportation mode is set to off with the first charging of the battery pack. After the first charging, the battery pack must be charged every 12 months. Store the battery pack with a charge of 40 - 60 % after the first charging.

Disposal

The additional battery must not be disposed of with household waste.

Observe the instructions for proper disposal (see chapter 14.2 Disposal of the battery).

Also see about this

Technical data [} 228]

17.6.1 Using the battery pack

Information

Before the first usage, the battery pack must be charged completely.

To use the battery pack, proceed as follows:

1) Plug in the charging cable to the socket for 24 V power supply at the battery pack.
2) Plug in the other end of the charging cable into the socket for external power supply at the hadnheld device.
3) Depending on the used accessories, attach the battery pack to the hand strap of the handheld device or the belt.

The battery pack is used.

KEBA © KEBA 2021

17.6.2 Charging the battery pack

Information

The battery pack can only be charged by the charging station at ambient temperatures < 40 °C.

To charge the battery pack, proceed as follows:

1) Attach the battery pack to the charging station using the magnet pad.
2) Plug in the charging cable into the socket for 24 V power supply at the battery pack.
3) Plug in the other end of the charging cable into the socket for 24 V power supply at the charging station.

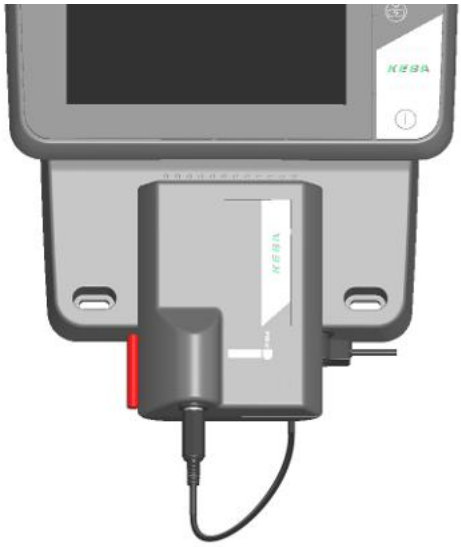


Fig. 17-111: Battery pack is charging at the charging station

The battery pack is charging.

The following must be observed:

- If the handheld device is attached to the charging station, always disconnect the battery pack from the handheld device.
- If the handheld device is attached to the charging station and the battery pack is connected to the handheld device, the battery pack does **not** charge.
- The charging station is not protected against reverse current from the battery pack. If the external supply to the charging station is switched off, the battery pack must be disconnected from the charging station, otherwise it will discharge unintentionally.

© KEBA 2021

17.6.3 Technical data

Environmental conditions

Operating temperature:	0 °C to 40 °C
Storage and transport temperature:	
• < 1 year	-20 °C to +20 °C
• < 3 months	-20 °C to +45 °C
• < 1 month	-20 °C to +50 °C
Charging temperature:	0 °C to 40 °C
Relative air humidity (non-condensing):	5 % to 95 %
Operating area:	Indoor
Installation altitude:	Max. 2,000 m above sea level
Protection type:	IP54
Pollution degree:	2

Voltages

Charging voltage:	24 V DC (nominal voltage tolerance range 19.2 V DC to 30 V DC SELV / PELV as of EN 61131-2)
Overvoltage category during charging:	II
Output voltage:	14.4 V DC

Operation and charing times

Typical operating time:	Approx. 3.5 h
Typical charging time to 80 % capacity:	Approx. 2 h

Mechanical properties

Construction:	PPE/PS housing
Flame retardance:	UL94-V0
Safe drop height (2 falls according to EN 61131-2):	1 m (on industrial floor), then at least protection class IP54

Dimensions, weight

Height:	50 mm
Width:	93 mm
Depth:	115 mm
Weight:	382 g

Battery Specifications

Model designation:	RRC2054
Battery category:	Device battery
Chemical composition:	Lithium-ion (Li-Ion)
Configuration:	4s1p
Capacity:	Approx. 3.4–3.5 Ah

KEBA © KEBA 2021

Rechargeable:	Yes
Replaceable	Yes

Cell Types Used

Cell type:	NCR18650GA	INR18650-35E
Cell manufacturer:	Panasonic	Samsung SDI
Capacity:	3.45 Ah	3.40 Ah
Energy:	49.68 Wh	48.96 Wh

17.7 Rear wall for cable installation on the back side (only for CB41x)

This accessory for CB41x can be used instead of the standard rear wall and enables wiring on the back side through an opening while the base station is closed.

Order number	Designation
106482	CB310 UT set for control cab. installation

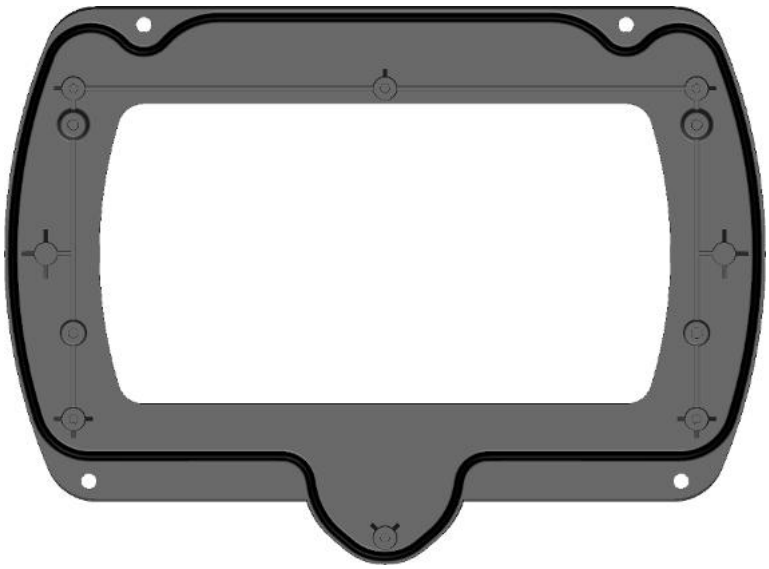


Fig. 17-112: Rear wall for wiring on rear

This rear wall is installed in the same way as the standard rear wall.

Caution

The installation surface of the rear wall, that is designed to be wired on the rear, is fitted with a seal. To guarantee the leak-tightness of the seal, it must be installed on an even surface and the cable feedthrough in the wall must be smaller than the opening in the rear wall.

© KEBA 2021

Caution

When the base station is wired with this rear wall, strain relief must be provided for the cables on the control cabinet side.

17.8 Tempered Glass Screen Protector

The following optional accessory is available for the handheld device to protect the display against scratches and damage:

Order Number	Description
140761	Premium Screen Protector Glass KeTop T15x

KEBA © KEBA 2021

18 Directives, standards and regulations

18.1 EU directives / Regulations

2014/53/EU	RED Directive
2022/30/EU	Delegated Regulation
2011/65/EU	RoHS Directive
2006/42/EG	Machinery Directive

18.2 Standards for checking the conformity

The following legally non-binding European standards were applied to checking conformity with the directives.

Verification of conformity with the RED directive

EN 300 328	Wideband transmission systems - Data transmission equipment operating in the 2.4 GHz band - Harmonized standard for use of wireless frequencies
EN 300 330	Short Range Devices (SRD) - Radio equipment in the frequency range 9 kHz to 25 MHz and inductive loop systems in the frequency range 9 kHz to 30 MHz - Harmonized EN covering essential requirements under Article 3.2 of the EU Directive 2014/53/EU
EN 301 893	5 GHz RLAN - Harmonized EN covering essential requirements under Article 3.2 of the EU Directive 2014/53/EU

Check of the conformity with the Low-voltage Directive (in accordance with RED Article 3 Paragraph 1a)

EN 50364	Product standard for human exposure to electromagnetic fields from devices operating in the frequency range 0 Hz to 300 GHz, used in Electronic Article Surveillance, Radio Frequency Identification (RFID) and similar applications
EN 62479	Assessment of the compliance of low power electronic and electrical equipment with the basic restrictions related to human exposure to electromagnetic fields (10 MHz to 300 GHz)
EN 62311	Assessment of electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (0 Hz to 300 GHz)

© KEBA 2021

Check of the conformity with the EMC Directive (in accordance with RED Article 3 Paragraph 1b)

EN 61131-2	Programmable controllers – Part 2: Equipment Requirements and Tests
EN 61000-6-2	Electromagnetic Compatibility (EMC) – Part 6-2: Generic Standards - Immunity for Industrial Environments
EN 61000-6-4	Electromagnetic Compatibility (EMC) – Part 6-4: Generic Standards – Emission Standard for Industrial Environments
EN 301 489-1	Electromagnetic compatibility (EMC) standard for radio equipment and services – Part 1: Common technical requirements

Check of the conformity with the Delegated Regulation 2022/30/EU (in accordance with RED Article 3 Paragraph 3b)

EN 18031-1	Common safety requirements for radio equipment (Part 1: Radio equipment with internet connection)

Check of the conformity with the RoHS Directive

EN IEC 63000:2018	Technical documentation for the assessment of electrical and electronic products with respect to the restriction of hazardous substances

Check of the conformity with the Machinery Directive

EN ISO 13850:2015	Safety of machinery - Emergency stop function - Principles for design
EN ISO 13849-1:2015	Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design
EN 60204-1:2018	Safety of machinery - Electrical equipment of machines - Part 1: General requirements
EN ISO 10218-1:2011	Robots and robotic devices - Safety requirements for industrial robots - Part 1: Robots
EN 62061:2021	Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems

18.3 Other standards

In addition, the following legally non-binding European standards were consulted in partial aspects during the development of the safety concept.

KEBA © KEBA 2021

General procedure and safety principles

EN ISO 12100:2010	Safety of machinery - General principles for design - Risk assessment and risk reduction

Stop or emergency stop execution

EN ISO 13850:2015	Safety of machinery - Emergency stop function - Principles for design
EN 60204-1:2018	Safety of machinery - Electrical equipment of machines - Part 1: General requirements

Design of the enabling switch

EN 60204-1:2018	Safety of Machinery - Electrical Equipment of Machines - Part 1: General Requirements
EN ISO 10218-1:2011	Robots and Robotic Devices – Safety Requirements – Part 1: Robots
EN 60947-1:2007	Low-voltage switchgear and controlgear - Part 1: General rules
EN 60947-5-1:2017	Low-voltage switchgear and controlgear - Part 5-1: Control circuit devices and switching elements - Electromechanical control circuit devices
EN 60947-5-8:2021	Low-voltage switchgear and controlgear - Part 5-8: Control circuit devices and switching elements - Three-position enabling switches

Ergonomics

EN 614-1:2006	Safety of machinery - Ergonomic design principles - Part 1: Terminology and general principles
EN 614-2:2000	Safety of machinery - Ergonomic design principles - Part 2: Interactions between the design of machinery and work tasks

Stability and impermeability of casing

EN 60529:1991	Degrees of protection provided by enclosures
EN 61131-2:2007	Programmable controllers - Part 2: Equipment requirements and tests

Functionally relevant electro-magnetic compatibility

EN 61000-6-7	Electromagnetic Compatibility (EMC) - Part 6-7: Generic Standards. Immunity Requirements for Equipment Intended to Perform Functions in a Safety-Related System (Functional Safety) in Industrial Locations

© KEBA 2021

EN 61326-3-1	Electrical equipment for measurement, control and laboratory use - EMC requirements - Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) - General industrial applications
EN 61131-6	Programmable controllers – Part 6: Functional safety
IEC 61131-2	Industrial-process measurement and control - Programmable controllers - Part 2: Equipment requirements and tests
EN 12895	Industrial trucks - Electromagnetic compatibility

Other relevant standards and principles

EN 61131-2:2007	Programmable controllers - Part 2: Equipment requirements and tests
EN 61010-1:2010	Safety requirements for electrical equipment for measurement, control, and laboratory use - Part 1: General requirements
EN IEC 61010-2-201:2018	Safety requirements for electrical equipment for measurement, control, and laboratory use - Part 2-201: Particular requirements for control equipment (without functional safety)
GS-ET-07	Wireless control equipment subject to safety requirements
GS-ET-22	Electromechanical enabling switches and enabling devices with and without start-up controllers
EN 62745:2017	Safety of machinery - Requirements for cableless control systems of machinery
EN 61508-1:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements
EN 61508-2:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
EN 61508-3:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements
EN ISO 3691-4:2020	Flurförderzeuge - Sicherheitstechnische Anforderungen und Verifizierung – Teil 4: Fahrerlose Flurförderzeuge und ihre Systeme
EN 61784-3-3:2017	Industrial communication networks - Profiles - Part 3-3: Functional safety fieldbuses - Additional specifications for CPF 3

KEBA © KEBA 2021

18.4 Regulations

Regulation (EG) No. 1907/2006	REACH EU chemicals regulation

Information

Information obligation from REACH regulation

To meet the information obligation according to article 33 of REACH regulation, detailed information to substances / SVHC are provided on our homepage. You can download the document directly from https://support.keba.com under "Regulations".

18.5 Standards for the American market

For the American market, the following standards were taken into account.

UL test for industrial control equipment

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, CFR 47, Part 15

CFR 47, Part 15	Radio Frequency Devices

The following radio modules are installed in the product:

Designation	FCC-ID	T15xWL	CB 4xx
RFID Uni Module	U87008	x	
Sparklan WPEQ	RYK-261ACNBT	x	
Ublox NINA B112	XPYNINAB1	x	x
Lantronix Xpico	R68XPICO200		x
WAL R1	U870009	x	x

The following information applies for the American market:

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.

© KEBA 2021

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 Standards for the Canadian market

For the Canadian market, the following standards were taken into account.

Radio Standards Specification RSS-210, Issue 8

RSS-210 Issue 8	Licence-exempt Radio Apparatus

The following radio modules are installed in the product:

Description	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.

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 Standards for the Japanese market

The following wireless modules are built into the product:

Designation	MIC-ID	T15xWL	CB 4xx
RFID Uni module	AC-21044	x	
Sparklan WPEQ	020-170122	x	

KEBA © KEBA 2021

Designation	MIC-ID	T15xWL	CB 4xx
Ublox NINA B112	204-610006	x	x
Lantronix Xpico	020-170133		x
WAL R1	203-JN1257	x	x

Also see about this

Certificate_Japan u-blox NINA-B111 NINA-B112 [} 238]

© 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

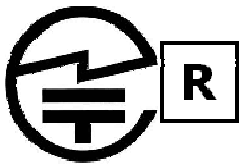
This certificate has 2 annexes.

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 Declaration of conformity

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): *Variant(s):*

Mat.Nr. KeTop T15xWL / C15xWL:

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

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 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 Appendix: Commissioning

This chapter describes the commissioning steps, some of which are described in the chapters with the same names.

1) Installing the base station.
2) Wiring the base station.
3) Configuration of the base station: Setting the box ID and, when using an operation area, setting this via the DIP switches.
4) Closing the base station and screwing it shut.
5) Validating the base station.
6) Optional: Installing and wiring the charging station.
7) Connecting the battery (the slot is open in delivery condition).
8) Closing the connection slot and screwing it shut.
9) Full charging of the handheld device on a charging device or the charging station (min. 2 h).
10) Connecting the handheld device to the base station ("Pairing").
11) Starting the device configuration ("DeviceConfig").
12) Configuring the base station using "Basestation".
13) Using "Network" to set the desired behavior ("Mode") and configure the network settings of the devices.
14) Configuring the handheld device (e.g. remote access, IT security settings)
15) Installing and configuring the desired connection protocols on the handheld device.
16) Configuring the visualization.
17) Load the visualization application onto the handheld device and start it.

KEBA © KEBA 2021

21 Appendix: Machinery safety

Guidelines of the European Union

An essential goal of the European Union is the realization of a single European market and thus free trade. This means that quantitative import limitations of goods between the member states are prohibited.

Goods that endanger the safety of persons or the environment are an exemption. Member states can prohibit such products in their country's territory. To ensure free trade for these products, the national safety regulations of the member states are standardized via guidelines set forth by the European Union.

These guidelines apply for a number of product classes, such as for example machines, medical products, as well as toys. However, corresponding guidelines were also developed for additional common safety aspects of products, such as protection against electricity, explosion protection or electro-magnetic compatibility. The guidelines are directed towards member states, who must implement them into the respective national laws. The guidelines therefore have legally binding effects.

With the CE label the manufacturer certifies to have met all obligations of the EC guidelines applicable for the product. The CE symbol, which is affixed to the products by the manufacturer itself, is the "passport" within the EU and intended for the overseeing authorities.

In addition, independent, accredited certification organizations can verify the conformity with the EU guidelines and confirm this with an EU design sample certification.

In addition to the Machinery Directive (MRL 2006/42/EC), the Radio Equipment Directive (RED RL 2014/53/EU) must also be applied for handheld devices due to the installation of radio modules.

Safety of machines

In all situations where faults occurring on the machine could cause personal injury or significant damage to machinery and equipment, additional external safety measures must be taken in order to ensure the system as a whole remains in a safe operating condition even in the event of a fault. According to the Machinery Directive (MRL), a machine is "an assembly of interconnected parts or devices, at least one of which is movable". The Directive also states that "the design of the machine must ensure that it can be operated, set up and maintained without endangering persons when used as intended."

Although the handheld terminal is not, strictly speaking, a machine, it does, however, perform important tasks to guarantee the safety functions of a machinery to which it is attached.

The handheld terminal has, for example, the "Emergency Stop" safety function and an enabling switch for use in special operating modes. It is, as a result, a “Safety Component" in the sense of the Machinery Directive.

© KEBA 2021

Safety components, i.e. parts whose failure or malfunction endangers the safety of persons in the danger zone of the machine, are expressly included in the scope of the Machinery Directive. Essential requirements of the Machinery Directive for the manufacturer of a machine or system are:

- Carrying out a hazard and risk analysis
- Following the principles for the integration of safety measures
- Creating and storing Technical Documentation
- Solutions in accordance with the state of the art of technology
- Presumption of conformity using harmonized standards
- Attachment of the CE conformity marking

The same requirements essentially apply to safety components. For safety components, it must be demonstrated that failure or malfunction is not possible, or that malfunction will not result in a hazardous situation.

21.1 Hazard and risk analysis

The manufacturer of a machine is required to analyze its machine throughout its operating life and in all modes of operation, and to document all hazards that may possibly arise. This has to be done without taking into account possible protection devices.

The next step is to formulate a goal for protection against each identified hazard and subsequently to define one or more protective measures to achieve the protection goal.

Further details about the procedure for carrying out the hazard and risk analysis and lists of commonly occurring hazards can be found in the following Standards:

- EN ISO 12100:2010 "Safety for machinery - General principles for design - Risk assessment and risk reduction "

21.2 Principles for the integration of KeTop

In Appendix I, Chapter 1.1.2 of the Machinery Directive 2006/42/EC there is a clear procedure and sequence for the selection of protective measures:

Eliminating or minimizing the hazards

This takes place at the design stage of the machine. These measures include, for example:

- A reduction in the use of energy (power, revolutions, voltages etc.) as far as this is possible
- The avoidance of unnecessary sharp points or edges
- The avoidance of human errors by means of the ergonomic and logical design of operating devices

KEBA © KEBA 2021

- The avoidance of hazardous materials and commodities

Taking protective measures against hazards that cannot be eliminated

These measures include, for example:

- Separating safeguard (guards, housings, railings)
- Non-separating safeguard (light barrier for hazard elemination)
- Protective control equipment (enabling switches, two-hand controls, speed monitoring etc.)

User information about residual hazards

This last of the three options is used if residual hazards remain after the first two options have been applied. These measures include, for example:

- Warning notices
- Training and organizational measures
- The use of personal protective equipment

21.3 Technical construction file

The technical construction file contains all the documents that are required to prove the safety of the machinery / safety component. These are, for example:

- A complete drawing of the machinery or safety component including control circuit diagrams
- Hazard and risk analysis
- Calculations
- Research and test results
- A list of the basic safety requirements of the Machinery Directive applicable to the machine and a description of the solutions
- Applied Standards
- Operating instructions
- A list of the quality assurance measures in the procedure

The technical construction file must be retained for a minimum of 10 years after the supply of the last product, and must be presented within a period of a few days in the event of a claim for damages.

© KEBA 2021

21.4 State of the art

This means technical possibilities at a certain point of time that are based on certain scientific and technical knowledge. The state of the art also means something that is commercially viable, that is it can be realized by the majority in the industrial sector concerned.

The state of the art is defined as the state of development of advanced procedures, equipment or operating methods, that makes the practical applicability of the measure appear assured overall in respect of the targeted goals (e.g. the goals of protection of work, protection of the environment, safety of third parties and operating efficiency: namely to achieve a generally high level overall in relation to the aspects under consideration).

The state of the art can develop further irrespective of the Standards.

21.5 Recognition of conformity by means of harmonized standards

The European Directives mainly contain general requirements for the safety of products; however they do not contain details of how to carry them out.

The European Standards Institutes are responsible for this. They provide implementation proposals for real safety problems or specific product classes. Standards that are assumed to meet and correctly interpret the requirements of the Directives are known as “Harmonized Standards”. Most of the available Standards, however, are not harmonized.

By applying and implementing harmonized Standards, a manufacturer can claim conformity for the respective product. However, the Standards, in contrast to the Directives, are not legally binding. This means that the manufacturer may also take into consideration other solutions that are not described in the Standards; but these solutions must attain at least the same safety level as the relevant Standards and satisfy the requirements of the appropriate Directives.

21.6 Selection of Performance Level and Safety Categories in accordance with EN ISO 13849-1

The Machinery Directive demands that a fault in control circuit logic, or interference or damage thereto, shall not lead to a hazardous situation.

This general approach is substantiated in EN ISO 13849-1 "Safety of machinery - Safety related parts of control systems", which defines Performance Levels (PL a to e) for control parts that are relevant to safety. The PL depends on the safety category, the $MTTF_D$-value and the degree of coverage of diagnosis (DC_{avg}) of the corresponding safety circuit.

As in the preceding standard EN 954-1, the safety category describes the structure of the safety function. The Performance Level (PL), which describes the conditional probability of failure and the defect discernibility of the safety function, has been added.

KEBA © KEBA 2021

The selection of the PL has to be done by the manufacturer of a machine depending on the real risk potential. The risk potential will be determined from a hazard and risk analysis. In case of hazards that can cause irreversible injury or death usually a Performance Level not less than PL d is required.

The category of the Performance Level determines if

- the system has been built in single circuit technology, which means that a failure will lead to a loss of safety, although the availability of components and parts is high (category 1)
- the system has been built in single circuit technology, which means that a failure will lead to a loss of safety, but the failure will be detected by the system and will be displayed somehow or other (category 2)
- the system has been built in multiple (2) circuit technology and that a fault will not lead to loss of safety (category 3) or
- the system has been built in multiple (2) circuit technology and a buildup of multiple faults will not lead to loss of safety (category 4).

Starting from category 3 it is also important in this context that individual faults are detected in time to avoid a buildup of faults, which may finally lead to loss of safety.

Faults that have to be detected in electric and electronic systems are for example short circuits between multiple circuits, interrupts, short circuits or contacts that are stuck together. Special certified safety control devices are often used to detect faults in the individual safety circuits, which have a certain PL. The PL quoted for these devices is only attained, however, if also the whole machine circuit under review lies within the scope of the respective PL and the PL of all components supporting the safety functions has to be considered. The PL must always be considered in relation to a complete safety function and not as applied to individual components or parts.

A guide for easily calculating the PL for a safety function consisting of several individual components can be found in standard EN ISO 13849-1 chapter 6.3 and appendix H and I.

If safety components are being connected in series, the individual component with the least PL determines the PL of the whole safety function. For example a safety function consisting of 3 components, one with category 4 PL e, another one with category 3 PL d and a third component with category 2 PL c will have a PL c for the whole safety function. This means that a fault will lead to loss of safety, although components with category 4 PL e are integrated into the safety function, as one of the components being used has category 2.

When chaining several PLs the overall PL can decrease. For more information read EN 13849-1 chapter 6.3..

The proof of attainment of a safety category can take place with the aid of an FMEA (Failure Mode and Effects Analysis), in which all the faults that could possibly arise are simulated, either theoretically or in practice, and it is demonstrated that the requirements of the category are fulfilled.

© KEBA 2021

21.7 Application of handheld terminals in special operating modes

For the manual control of machines in special operating modes, where safety depends on the timely reaction of the operating staff, it is absolutely essential that the operator can overlook the operating area. The handheld terminal has the advantage that the operator can get very close to the control panel. At the same time, the danger of misuse increases with mobility since, in remote locations where it is not possible to observe the operating area, machine movements can also be set in motion with the handheld terminal, knowingly or unknowingly. The machine operator, therefore, has to find the right compromise between necessary flexibility and a reasonable limitation of the working range when selecting the corresponding cable length for the handheld terminals. It is not possible for the working range of radio-operated handheld terminals to be limited by means of the cable; therefore additional technical solutions are required for these handheld terminals.

If the machine or equipment is operated with the handheld terminal, care must be taken at this time to ensure that operation can only be controlled by the handheld terminal and cannot be operated from any other point on the equipment. The hazard zone may only be entered by the person who is operating the handheld terminal. If it should be necessary for more than one person to work in the hazard zone at the same time, each person present requires an enabling switch and machinery movement may only be allowed after all the enabling switches have been activated.

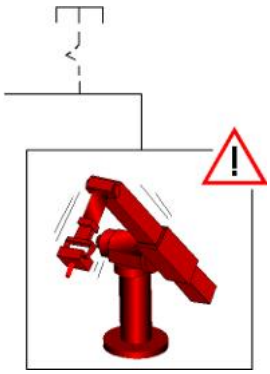
21.8 Information about the emergency stop button

In theory, a perfectly designed machine should not require an emergency stop button, since the Machinery Directive demands that a machine must be safe throughout its lifetime and in all operating modes.

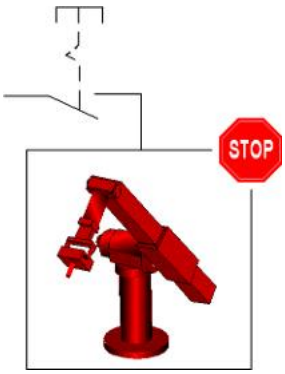
In practice, however, one is aware that unforeseen situations arise, in spite of all precautions. In order to enable fast shutdown of the machine in these cases, or to avert danger, an emergency stop button is provided on most machines.

As can be seen from the following illustration, a machine is permanently in the hazard state from the viewpoint of the emergency stop button, for as long as this is not activated.

KEBA © KEBA 2021



Neutral position (not activated)



Emergency stop button pressed

The emergency stop button may not, therefore, serve as the primary safety device but is provided exclusively to cover any residual risks.

Instead of this and depending on the mode of operation, other methods should be employed as the primary safety device, for example guards, light barriers and two-hand control devices or enabling switches.

When the emergency stop button is activated, the entire machine or all of the machines that are switched together in a plant must be lead to a safe state e.g. by stopping and switching off the power to the endangering drive mechanisms (stop categories 0 or 1 in accordance with EN 60204-1).

The release of the emergency stop button must not cause any uncontrolled restart of the machine.

Irrespective of whether a handheld terminal has an emergency stop button or not, permanently installed, universally identifiable and easily accessible emergency stop buttons must be provided at selected points around the machine in every case.

21.9 Manual control of machines in special operating modes

The machinery directive does not place any detailed requirements on the coloring of the operating elements for stopping in an emergency. The requirement is as follows: "The emergency switch must have easily recognizable, clearly visible and rapidly accessible control devices".

Normally, "emergency stop" buttons are marked red-yellow. The special design has the meaning of a signal and is intended to enable everyone, but especially untrained persons, to quickly recognize the operating element as the device used to eliminate a danger in an emergency.

Therefore, an absolute requirement is that devices marked in this way can be used to initiate a safe state at all times and in any operating mode, without further knowledge of the machine (see also EN ISO 13850). Changing operating readiness of an emergency stop button is not permitted, since this can lead to misuse and life-threatening loss of time in panic situations.

© KEBA 2021

Illuminated emergency-stop

Wireless handheld devices are intended for frequent changes of operation between one or more machines and are only needed there temporarily, for commissioning or setup work.

Various measures, such as the CB4xx, base station, are used to bypass the emergency stop circuits of the machine when the handheld device is not connected, so that the machine can continue to run in normal operation even without the handheld device. The machine can then be started and operated via an independent operating device.

Due to the frequent change of operation of the manual control units, it cannot be ruled out that unpaired manual control units with ineffective emergency stop functions are lying or hanging in the meantime in the vicinity of machines in operation and are mistaken for functioning devices in emergency situations.

The approach of giving preference to the constructive elimination of the hazard by means of unambiguous coloring, over any organizational measures, also corresponds to the "Principles for the integration of safety" of the Machinery Directive already described above, and is therefore mandatory by law.

For this reason, wireless handheld devices may be equipped with an illuminated emergency stop switch only. Changing the color by illuminating the active emergency stop switch avoids confusion between handheld devices with an active and inactive emergency stop switch.

Information

If emergency stop switches are mounted on wireless operator stations (e.g. portable programming devices), then at least one device with a (red yellow) emergency stop must always be available wired (stationary) on the machine!

21.10 Information about enabling switches

Many machines have both a normal and special operating modes.

The machine fulfills its primary mission in normal (automatic) operation. In this mode of operation, safety is guaranteed by closed, guards and/or with protective devices.

A machine’s special operating modes serve to maintain normal operation. In doing so, safety must be guaranteed in a way that is different to normal operation, since hazardous areas of the machine can now be entered and targeted machine movements have to be possible. The enabling switch plays a primary role here.

KEBA © KEBA 2021

This application requires the enabling switch to eliminate the hazards that are to be controlled in a timely manner, before any personal injury occurs. Additional safety measures may be necessary for this purpose, such as safely reducing the speed of drive mechanisms.

In contrast to the emergency stop button respectively the stop button, a machine in special operating mode with an enabling switch is in a safe state as long as this enabling switch is not activated (see illustration).

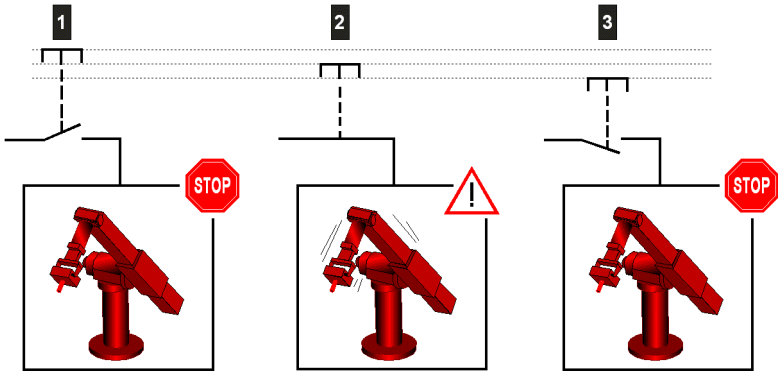


Fig. 21-113: Enabling functions

1 ... "Neutral position" not activated	2 ... "Enabling" pressed
3 ... "Panic" pressed heavily	

The enabling function is also described in EN 60204-1 and corresponds to the state of the art.

The panic position on 3 stage enabling switch was introduced because limbs often become cramped when a person is in a state of shock and as a result is not able to release the enabling switch. For this reason, firmly pushing down on the enabling switch also leads to switch off.

The controller must be designed in such a way that machine movement is not initiated directly when the enabling switch is activated but only as a result of the additional activation of a control button. This may be via the handheld terminal's membrane keyboard or graphical software buttons on the touch screen.

An optionally available joystick can also be used to trigger the machine movement signal.

According to EN 60204, only stop categories 0 or 1 are allowed for the enabling function, i.e. stopping the machine with the enabling switch must always be combined with switching off the power supply to the drive mechanisms.

In order to prevent incorrect, permanent activation of the enabling switch by mechanical fixing devices, it is recommended to limit the maximum duration of an accepted enablement. This must be achieved by means of a controller located downstream to the handheld terminal.

© KEBA 2021

An enabling switch is not a replacement for a two-hand control device, which is specified for some machines (e.g. presses) and must therefore not be confused.

In contrast to the enabling switch, the two-hand control device forces the endangered limbs of the operator into a safe position whilst the machine is in motion.

KEBA © KEBA 2021

22 Appendix: Chemical resistance

The following table shows an overview of the general chemical resistance of the materials used in the T15xWL. The list is eventually not exhaustive.

Due to the strong creep characteristics of some substances those can get harmfully into the device and into components. This kond of resistance is not assessed.

The given values refer exclusively to laboratory tests. The used materials are often subjected to influences which can not be detected in laboratory tests (temperature, pressure, humidity, etc). The given values only serves as guideline. In cases of doubt, it is recommended to perform a test.

In the subsequent table the materials are abbreviated as follows:

G/S:	Housing + slot cover
T:	Keyboard
AB:	Hanging bracket
TS:	Touchscreen
H:	Hand strap
NH:	Emergency stop
ZT:	Enabling switch
USB:	USB
AK:	Connection cable

The resistance of the materials are distributed into the following classification:

\+ Good resistance o Limited resistance - Bad resistance

Medium	G/S	T	AB	TS	H	NH	ZT	USB	AK
Acetone CAS no.: 000067-64-1 Concentration: -	o	+	+	+	+	+	+	o	+
Ammonia CAS no.: 001336-21-6 Concentration: 10%	+	+	+	+	+	+	+	+	+
Gasoline CAS no.: 086290-81-5 Concentration: -	+	+	+	+	+	+	+	+	+
Diesel CAS no.: - Concentration: -	+	+	+	+	+	+	+	-	+
Acetic acid CAS no.: 000064-19-7 Concentration: 10%	+	+	+	+	+	+	+	-	+
Ethanol CAS no.: 000064-17-5 Concentration: 95%	+	+	+	+	+	+	+	+	+

© KEBA 2021

Medium	G/S	T	AB	TS	H	NH	ZT	USB	AK
Hydraulic oil (mineral oil-based) CAS no.: - Concentration: -	+	+	+	+	+	+	+	o	+
Potassium hydroxide CAS no.: 001310-58-3 Concentration: 10%	+	+	+	+	+	+	+	o	+
Linseed oil CAS no.: 008001-26-1 Concentration: -	+	o	+	+	+	+	o	o	+
Cutting/Grinding oil CAS no.: - Concentration: -	+	o	+	+	+	+	o	o	+
Methanol CAS no.: 000067-56-1 Concentration: -	+	+	+	+	+	+	+	+	+
Methylbenzene (toluene) CAS no.: 000108-88-3 Concentration: -	+	+	+	+	+	+	o	-	+
Methyl ethyl ketone (butanone) CAS no.: 000078-93-3 Concentration: -	o	o	o	+	+	+	o	-	o
Motor oil CAS no.: - Concentration: -	+	o	+	+	+	+	+	o	+
Sodium hydroxide CAS no.: 001310-73-2 Concentration: 10%	o	-	+	o	+	+	+	+	o
Petroleum ether (light gasoline) CAS no.: 008032-32-4 Concentration: -	+	+	+	+	+	+	+	+	+
Hydrochloric acid CAS no.: 007647-01-0 Concentration: 10%	+	+	+	+	+	-	+	-	o
Grease CAS no.: - Concentration: -	+	o	+	+	+	+	+	+	+
Sulfuric acid CAS no.: 007664-93-9 Concentration: 10%	+	+	+	+	+	+	o	o	+
Silicone oil CAS no.: - Concentration: -	+	+	+	+	+	+	+	+	+
Ethyl alcohol CAS no.: - Concentration: -	+	+	+	+	+	+	+	o	+
Turpentine CAS no.: - Concentration: -	+	+	+	+	+	+	+	-	+

KEBA © KEBA 2021

23 Appendix: Terms and definitions

The terms and definitions in this document are based on IEC 62443.

System owner

An asset owner is an individual or a company that is responsible for an IACS. An asset owner can be responsible for one or more IACS.

Boundary protection device

The device that securely connects the networks is a "boundary protection device". The boundary is the contact zone of these networks. The boundary protection device enables partitioning into separate zones. These separate zones are part of a defense in depth strategy. They are also important for the threat and risk assessment of a system.

IACS

IACS is the abbreviation for "Industrial Automation and Control System". The term IACS covers systems that influence or affect the safe and reliable operation of industrial processes. It includes industrial control systems such as PLCs with communication networks, which are the focus of this document.

Integrity

Integrity reflects the logical correctness of a system, the logical completeness of hardware and software and the consistency of data.

Product family

A group of products that have a common area of application and related functions.

Availability

The probability that an object will fulfill a required function at a certain point in time. It is assumed that the required environment and resources are available.

Confidentiality

Protection against the disclosure of information to unauthorized persons and institutions.

© KEBA 2021

Index

A

Ambient conditions
- Technical data 198

B

Battery pack 223

Box ID
- Address switch position 137
- Configuration 137

Bumper
- Order number 217

C

Cable outlets
- Technical data 92, 112, 130

CNC-Tastatur 73

Configuration
- Device configuration 140

Connection detection
- Wiring..... 94, 114, 131

D

Dimensions
- Technical data 204

E

Emergency stop
- Position..... 83
- Wiring 93

Emergency stop configuration
- LED position 83

Emergency stop function
- Technical data 207
- Wiring 93

Enabling control
- Normal operation..... 80
- Panic operation 80

Enabling switch
- Technical data 206

Environmental conditions
- Technical data 215, 217

Ethernet
- General..... 97, 115, 133
- Status LED position..... 83
- Wiring 97, 115, 133

Ethernet interface
- Pin assignment..... 98, 115, 133

Extra battery
- accessories 224
- Service life..... 226
- storage 226

F

Flash storage medium 176

Folientastatur
- CNC-Tastatur 73

KEBA © KEBA 2021

G
General
Technical Data 198, 202

I
Illuminated pushbutton
Position 83
Interfaces
Technical data 203, 204, 205

K
Kabelauslässe
Position 84
Key management 171
Key mapping 171
Key-operated switch
Wiring 94, 114, 131
Keypad
Robotics keypad 72
Standard keypad 71

M
Mechanical properties
Technical data 201
Membrane keypad
Robotics keypad 72
Standard keypad 71
Micro SD interface
Technical data 203

P
Power button 177
Power supply
Technical data 202
Power-LED
Position 83
Processor 202
PS/2 code 171

R
RFID
Technical data 203
Robotics keypad 72

S
Schnittstellen
Technische Daten 205
Shut down 176
Signalsäule
Verkabelung 95, 114, 132
Standard keypad 71
Status LED bar
Error states 188
General 87, 107, 125
Operating statuses 177
Position 83
Switch off 176

T
Tastatur
CNC-Tastatur 73
Trageset
Bestellnummer 219
Typenschild
Position 85

U
USB interface
Technical data 203

V
Voltage supply
Technical data 204
Wiring 93, 113, 131

W
Weight
Technical data 204

© KEBA 2021

Z

Zusatz-Akku
Bestellnummer 225

KEBA © KEBA 2021