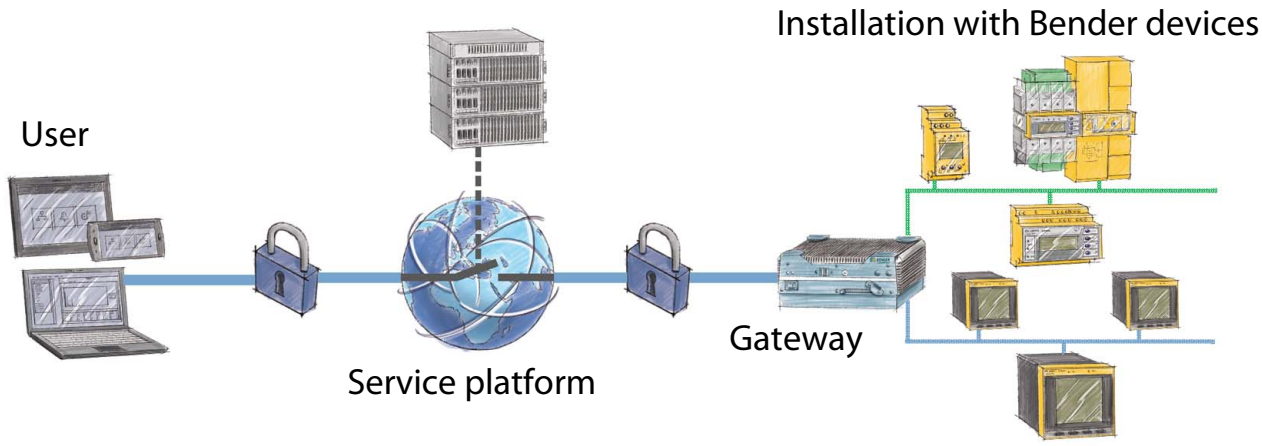
EN Manual

Bender Remote Assist



BRA_D00175_00_M_XXEN/01.2016

Bender GmbH & Co. KG
P.O. Box 1161 • 35301 Gruenberg • Germany
Londorfer Straße 65 • 35305 Gruenberg • Germany
Tel.: +49 6401 807-0 • Fax: +49 6401 807-259
E-mail: info@bender.de • www.bender.de

Photos: Bender archives.

Table of Contents

1. How to get the most out of this manual 7

1.1 How to use this manual 7

2. Safety instructions 9

2.1 Work activities on electrical installations 9

2.2 Intended use 9

2.3 Delivery conditions, warranty and liability 9

3. Product description 11

3.1 Scope of delivery 11

3.2 Characteristics 11

3.3 Functional description 11

3.3.1 The hardware 12

3.3.2 The software 12

3.3.3 The service 12

4. Mounting and connecting the COM700RA gateway 13

4.1 Scope of delivery 13

4.2 Warning instructions 13

4.3 Preliminary considerations 14

4.4 Installing the device 14

4.5 Connecting the device 15

4.5.1 BMS bus, Modbus RTU 16

4.6 Switching on the device 17

4.7 Creating system conditions for web user interface 17

4.8 Commissioning 18

5. Setting up the software 19

5.1 Creating system conditions for web user interface 19

5.2 Installing the software "OpenVPN" 19

5.3 Configuring the software "OpenVPN" 20

5.4 Setting up or terminating an OpenVPN connection 20

5.4.1 Setting up an OpenVPN connection 20

5.4.2 Terminating an OpenVPN connection ... 20

6. Service platform ... 21

6.1 Features service platform ... 21
6.1.1 Security ... 21
6.1.2 Remote access ... 22
6.1.2.1 Setting up a remote access connection ... 22
6.1.2.2 Terminating a remote access connection ... 22
6.1.3 Link check ... 23
6.1.4 Installation status ... 23
6.1.4.1 Status values and status display ... 23
6.1.4.2 Alert in the event of status change ... 24
6.1.5 Reports ... 24
6.1.5.1 Connection reports ... 24
6.1.6 Alerts and notifications ... 25
6.1.6.1 Alarm groups ... 25
6.1.6.2 Alarm condition ... 25
6.1.6.3 Notification ... 25
6.1.6.4 Contacts ... 26
6.1.7 Installation documentation ... 26
6.1.7.1 Documents and files ... 26
6.1.7.2 Logbook ... 26
6.2 Using the service platform ... 27
6.2.1 Logging in as a user with password ... 27
6.2.2 The "Installations" window ... 27
6.2.2.1 Displaying installation details ... 28
6.2.2.2 Setting up a connection ... 28
6.2.2.3 Using the logbook ... 28
6.2.2.4 Displaying documents ... 29
6.2.2.5 Displaying messages/alarms ... 29
6.2.3 The "status" window ... 30
6.2.4 The "reports" window ... 30
6.2.5 User settings ... 30
6.2.5.1 Displaying my settings ... 30
6.2.5.2 Changing my settings ... 30

7. Using the web user interface of the COM700RA ... 31

7.1 Basic information regarding the web user interface ... 31
7.1.1 Devices compatible with COM700RA ... 31
7.1.2 Functions available via the web user interface ... 31

7.2 Operating the web user interface 32

8. Data, terms, troubleshooting 33

8.1 Technical specifications COM700RA 33
8.2 Ordering information 33
8.3 Standards, approvals, certifications 33
8.4 Disposal 34
8.5 Terms used 34
8.6 Troubleshooting 35
8.6.1 Damage in transit 35
8.6.2 Malfunctions 35
8.6.2.1 What should be checked? 36
8.6.2.2 Where to find help? 36

INDEX 37

1. How to get the most out of this manual

1.1 How to use this manual

This operating manual is intended for skilled persons in electrical engineering and communication technology!

Explanatory comments regarding terminology and requirements can be found in the chapter "Terms used" on page 34.

To make it easier for you to understand and revisit certain sections of text and instructions in the manual, we have used symbols to identify important instructions and information. The meaning of these symbols is explained below:

*The signal word indicates that there is a **high** risk of danger that **will** result in **death** or **serious injury** if not avoided.*

*This signal word indicates a **medium** risk of danger that **can** lead to **death** or **serious injury**, if not avoided.*

*This signal word indicates a **low level** risk that can result in minor or **moderate injury** or **damage to property**, if not avoided.*

This symbol denotes information intended to assist the user in making optimum use of the product.

2. Safety instructions

2.1 Work activities on electrical installations

DANGER

Risk of fatal injury from electric shock

Any work on electrical installations which is not carried out properly can lead to death and injury!

► *All the work necessary to install, commission and operate a device or system is to be undertaken by appropriately skilled persons.*

- Compliance with applicable regulations governing work on electrical installations and with the regulations derived from and associated with them, is mandatory. EN 50110 is of particular importance in this regard.
- If the device is being used in a location outside the Federal Republic of Germany, the applicable local standards and regulations must be complied with. The European standard EN 50110 can be used as a guide.

2.2 Intended use

The service product "Bender Remote Assist" consists of hardware, software and Bender service. The operator as well as Bender service can access an installation containing Bender devices via a secure Internet connection to read out information or change settings.

"Bender Remote Assist" has been designed, developed and produced for normal use in the industrial sector. It has not been designed for use bearing high risks and dangers, which can result in death, injury, serious physical harm or any other loss unless exceptionally high safety measures are ensured.

CAUTION

The device is only suitable for use in the industrial sector. The emissions of the device may exceed the permissible limits for residential, business or commercial areas or small companies.

2.3 Delivery conditions, warranty and liability

The conditions of sale and delivery set out by Bender apply.
Conditions of sale and delivery can be obtained from Bender in printed or electronic format.

The five-year guarantee "5forU" does not include parts subject to wear, e.g. the battery of the gateway.

3. Product description

3.1 Scope of delivery

You will receive:

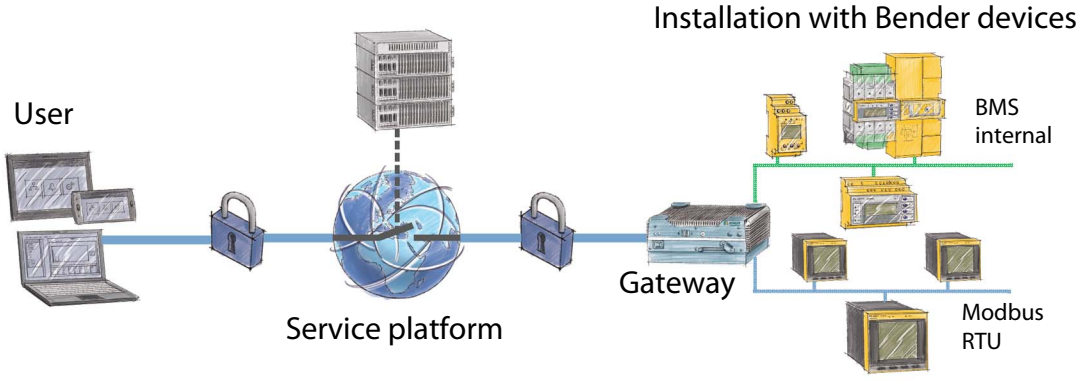
- the gateway COM700RA with accessories
- this manual as a PDF file (download)
- software to set up the access to the service platform (download)
- Login details for the service platform
- Bender service according to your order

3.2 Characteristics

- Continuous installation monitoring by the operator and/or Bender service
- Remote diagnosis allows fast support in the event of a fault
- Remote maintenance for early detection of faults prevents failures
- Remote access via LAN, WAN or the Internet
- High level of security due to VPN technology (Virtual Private Network)
- Easy operation via any Internet browser
- Password administration for different access rights
- Selective e-mail notification in the event of alarms
- Communication with Bender devices that are connected to the internal BMS bus via Modbus RTU or Modbus TCP (universal measuring devices, RCMS, Isometer, EDS systems)
- Parameter setting of devices, storing, documentation and restoring of parameters in a clear and practice-oriented manner
- Indication and visualisation of device and installation statuses
- Introduction of third-party equipment possible after test

3.3 Functional description

The service product "Bender Remote Assist" consists of hardware, software and Bender service. The operator as well as Bender service can access an installation containing Bender devices via a secure Internet connection to monitor, document and analyse.



3.3.1 The hardware

The gateway COM700RA links the service platform to the installation containing Bender devices.

The gateway provides a uniform web user interface for the devices assigned via different interfaces (max. 247 devices). In order to be able to identify them, one individual address is available for each device on this interface. BMS and Modbus RTU devices receive the address necessary for their interface. A virtual address is assigned to Modbus TCP devices.

The gateway generates and saves a process image from the communication with the devices assigned. This process image contains all alarms, status information and measured values of the assigned devices.

3.3.2 The software

The service platform offers a high level of security, which goes beyond the well-known security of VPN connections. The software and the database of the service platform are located on the servers of a data centre (hosted by the Telekom in Berlin). This data centre provides maximum availability and security standard around the clock.

Only the service platform can establish a connection between user and the installation containing Bender devices. It administrates the users (operator and/or Bender service) and their access rights. It also administrates the connected installations and informs about status and availability.

3.3.3 The service

You will receive the login details for the service platform. Depending on the booked package, different services are available, as for example remote maintenance, fault diagnosis, visualisations, discounts on an on-site service and many more. For a precise overview of the service components and packages please contact your personal Bender advisor.

Situation	Service
Operating error, incorrect parameters	Bender service detects the error via remote access and corrects it.
Hardware fault undetectable	Bender service reads out the history memory of the device and locates the fault.
Imprecise fault description	Bender service accesses installation and fault data directly and locates the fault. Misunderstandings and reporting errors due to oral transmission of information can be avoided.
The personnel in charge is not available or not on site.	The personnel can remotely access the installation or Bender service technicians can assist.
Defective device	Bender service either sends a replacement device or, because they have been able to remotely identify the problem, completes on-site repairs with only one visit (a second visit is therefore not required).
The installation is operative, failures should be avoided	Bender service carries out regular tests on the installation status. In the event of unusual results, the necessary measures are immediately taken.

4. Mounting and connecting the COM700RA gateway

4.1 Scope of delivery

Together with the COM700RA you will receive:

- a quick reference guide
- a pluggable screw terminal for the power supply
- two RS-485 cables for connection to the BMS bus and the Modbus RTU, 2 m long
- two terminating resistors each for the BMS bus and the Modbus RTU
- a DIN-rail mounting kit

4.2 Warning instructions

DANGER

Risk of fatal injury from electric shock

Parts of the system are live. During installation and connection:

- ► *Do not touch parts of the system.*
- ► *Electrically isolate the installation and secure it against unintentional switch on.*

WARNING

Warning: Risk of destruction due to incorrect mains voltage

- ► *Refer to nameplate for permissible mains voltage.*

DANGER

Mortal danger and risk of irreparable damage due to moisture!

- ► *Install device in such a manner that it is protected against moisture.*

WARNING

Malfunction due to double address assignment

Assigning addresses that are already used by existing devices in the BMS or TCP/IP networks concerned may cause serious malfunctions.

CAUTION

Do not remove CompactFlash card

- ► *Do not remove the CompactFlash card in order to ensure that all device properties are available!*
- ► *If a replacement of the CompactFlash card becomes necessary, you have to disconnect the device from the power supply.*

WARNING

Warning: Risk of destruction due to heat accumulation

- ► *Do not cover ventilation slots!*

If you are familiar with the configuration of computer networks, you can carry out the connection of the COM700RA yourself. ***Otherwise please contact your EDP administrator!***

4.3 Preliminary considerations

1. Have all the questions as regards the installation been answered by the technician responsible for the installation?
2. Is the BMS address to be set known?
   Can the COM700RA be operated as the master (BMS address 1)? If, apart from the COM700RA, an alarm indicator and test combination MK800 is connected to the internal bus, the COM700RA must **not** have the address 1 (master).
   You will find more detailed information on the BMS topic, in particular about the wiring of bus devices, in the separate document "BMS bus". You can download the document from the download area of the website www.bender.de.
3. Does the computer network comprise a DHCP server?
   Otherwise, the network data such as the IP address and net mask allocated by the person responsible for the electrical installation have to be set manually.
4. Ask for the IP address of the NTP server, which is required for automatic time setting.
5. Are suitable PC hardware and software available for commissioning?
   Minimum system requirements: 1.6 GHz processor/512 MB RAM/
   Windows XP/Vista/7/web browser with Microsoft Silverlight™ (version 5.0 or higher).
   System requirements (recommended): Dual-core processor/1024 MB RAM/
   Windows XP/Vista/7/web browser with Microsoft Silverlight™ (version 5.0 and higher)

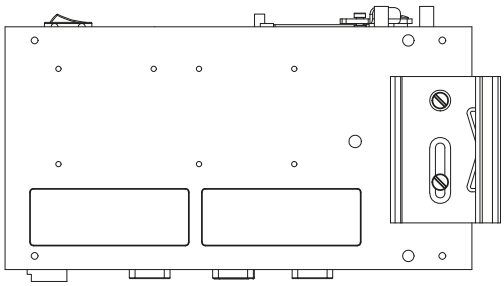
For initial connection, the basic configuration of the COM700RA is to be undertaken outside the installation, depending on the specific situation.

4.4 Installing the device

The general safety conditions as well as the prevailing national accident prevention regulations are to be adhered to. Electrical installation is to be carried out according to all applicable local laws. The climatic conditions must be complied with. The device is only permitted to be used in closed rooms.

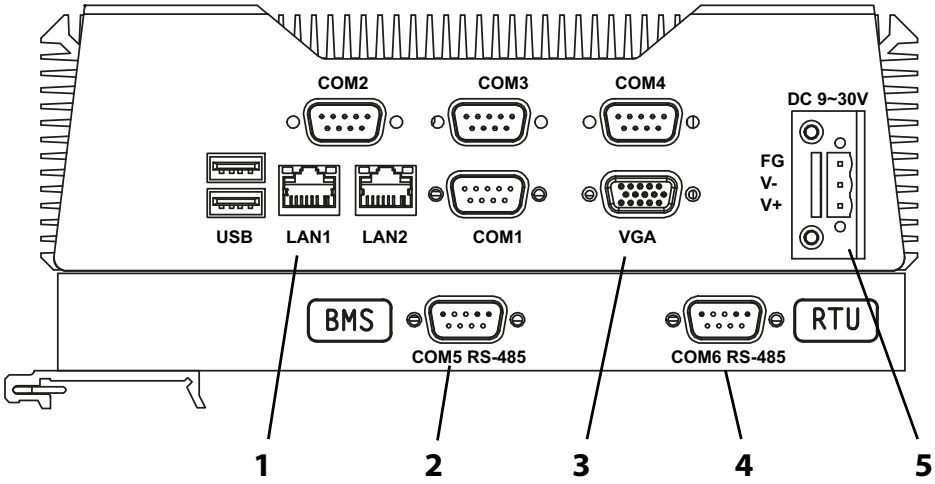
DIN rail mounting according to IEC 60715

1. Fasten DIN-rail mounting plate to the COM700RA using the screws (S) supplied with the device.



2. Mount device on DIN-rail.

4.5 Connecting the device



1	LAN1: Ethernet 10/100/1000, RJ45 socket for connection to PC or local network (hub, switch, router).
2	BMS bus (Bender measuring device interface)
3	VGA connector: displays status information only (IP address).
4	Modbus RTU interface.
5	Connect supply voltage and functional earth.
The sockets COM1, COM2, COM3, COM4, USB and LAN2 are not used	

Connection

1. Plug the RJ45 cable in the socket "LAN1" for connection to PC or LAN (**1**)
2. Plug in RS-485 cable for connection to the BMS bus (**2**) and the Modbus RTU (**4**). Connect corresponding terminating resistors
3. Connect voltage supply DC 24 V and functional earth (**5**). Recommended power supply: ABB, type 1SVR427044R0200/CP-D 24/2.5, EAN: 4016779661188.

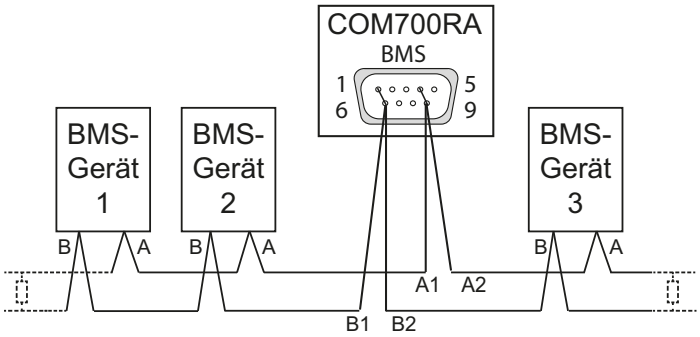
4.5.1 BMS bus, Modbus RTU

The two connecting cables (RS-485 cable) are included in the scope of delivery of the COM700RA. The double cable ends facilitate the connection of the device if it is arranged in the middle of the bus. Both cables have the same pin assignment.

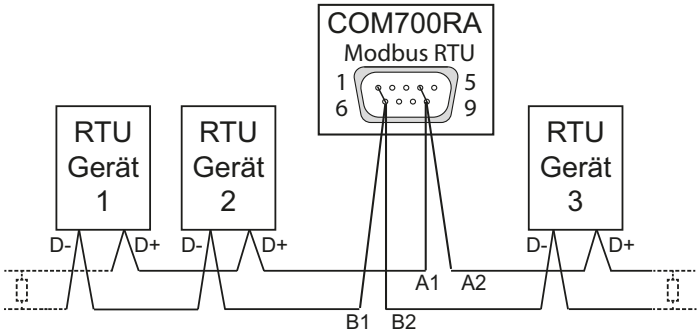
Plug connector	Loose cable ends	Core colour	Connection to the BMS bus	Connection to the Modbus
Bridge 4--9	A1	White	A	D+
	A2	Yellow		
Bridge 1--6	B1	Brown	B	D-
	B2	Green		
Not connected	Shield	Black	Shield	Shield

Wiring examples

BMS bus



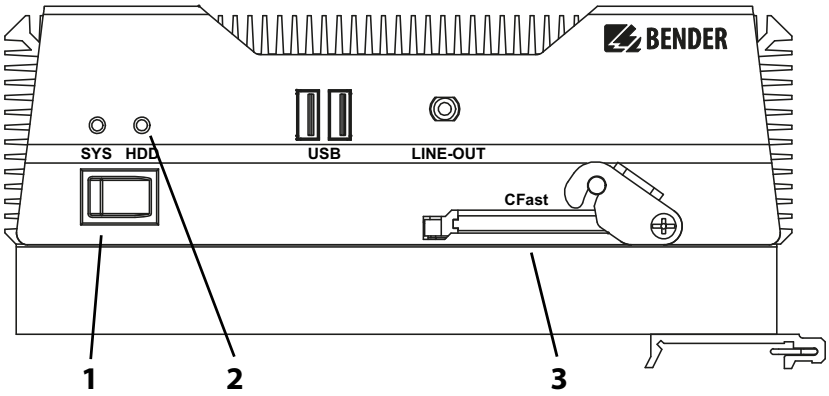
Modbus RTU



4.6 Switching on the device

Switch the supply voltage on. - The LED "SYS" lights in green.

Operating elements



1	"Power" button The device starts as soon as supply voltage is applied. The button is only necessary to carry out a reset (press button briefly) or to switch off the device (press button long).
2	SYS: LED lights • Red in the event of an error • Green when the device receives voltage supply • White when the device is switched off HDD: LED indicates access to internal flash hard drive.
3	CompactFlash slot with locking function.
The USB and LINE-OUT sockets are not in use.	

CAUTION

*Do not remove the CompactFlash card in order to ensure that **all** device properties are available!*
If a replacement of the CompactFlash card becomes necessary, you have to disconnect the device from the power supply.

4.7 Creating system conditions for web user interface

System conditions PC

- Web browser
- Microsoft Silverlight (version 5.0 or higher) must be installed.
- JavaScript should be activated; e.g. required for report and software update.
- Pop-up blocker should be deactivated for the IP address of the COM700RA. Otherwise, it would interfere with the software update request and the network settings.

4.8 Commissioning

1. For initial connection to device: use fixed IP address 169.254.0.1.
2. Set local IP address of the COM700RA.
3. Enable port: 1194 (UDP, direction: outgoing) in the firewall of the customer installation for the local IP address of the COM700RA.
4. Set BMS bus address of the COM700RA.
5. Carry out NTP/time setting

CAUTION

Malfunction due to incorrect NTP/time setting
In the event of incorrect setting, accessing the service platform is not possible. Pay attention to correct setting or contact Bender service.

5. Setting up the software

5.1 Creating system conditions for web user interface

- Operating system: Windows 7 SP1 (32 /64 bits), Windows 8.1 (32 /64 bits). Recommended: 64 bits.
- Rights: administrator
- Hard disk space: 10 MB
- The physical IP address of the PC in a network as well as the corresponding network may **not** contain the following address ranges:
  - 10.0.0.0/24
  - 10.1.0.0/16
  - 172.31.0.0/16
- To set up the VPN connection, the port 80 to the domain name of the Remote Assist server (bender.mcdialog.net, IP address 212.91.241.247) must be opened (outgoing) for the TCP protocol in all firewalls of the Internet connection of the PC!
- The OpenVPN connection (TCP to bender.mcdialog.net (212.91.241.247), port 80) must **not** be directed via a proxy!
- To access the Bender Remote Assist platform, the following IP address ranges may **not** be directed via a proxy:
  - 10.0.0.0/24
  - 10.1.0.0/16
    (Please also adjust the settings in the browser!)

5.2 Installing the software "OpenVPN"

The software "OpenVPN" is an open source project and can be used in compliance with the GPL licence terms (refer to https://openvpn.net/index.php/terms-of-use.html.

1. Open Internet browser and go to the download page:
   https://openvpn.net/index.php/open-source/downloads.html
2. Select the installation file according to your operating system:
   - 64-bit operating system: "openvpn-install-2.3.x-I001-x86_64.exe"
   - 32-bit operating system: "openvpn-install-2.3.x-I002-i686.exe"
3. Follow the installation instructions. Install the file in the Windows program directory with the suggested folder name "OpenVPN".

The installation sets up a new network connection (TAP-Win32 adapter).
Please check whether the network connection has been set up!

5.3 Configuring the software "OpenVPN"

You will receive the files required for installation as a ZIP file. It contains:

- a configuration file (ending .ovpn).
- a folder with 3 files:
  - the CA certificate,
  - the client certificate,
  - the client key.

Procedure:

1. Unpack the ZIP file.
2. Copy configuration file (ending "ovpn") to the program directory in the subfolder "…\OpenVPN\config"
3. Copy folder (containing the three files) to the program directory in the subfolder "…\OpenVPN\config"

5.4 Setting up or terminating an OpenVPN connection

5.4.1 Setting up an OpenVPN connection

1. Start the program "OpenVPN GUI"
   (via the start menu (Windows 7) or via the app overview (Windows 8.1).
   - The symbol  appears in the task bar.
2. **Right-click** on the symbol  . - The context menu appears.
   - Select the entry that matches the configuration file name "xxx.ovpn". - Another menu will appear.
   - **Left-click** on "Connect".

The VPN connection is set up. After successfully setting up the VPN connection, the symbol in the task bar is shown in green  .

If no connection can be set up, the program "OpenVPN GUI" must be started with the option "run as administrator".

5.4.2 Terminating an OpenVPN connection

1. **Right-click** on the symbol  . - The context menu appears.
   - Select the entry that matches the configuration file name "xxx.ovpn". - Another menu will appear.
   - **Left-click** on "Connect".

6. Service platform

6.1 Features service platform

6.1.1 Security

Bender Remote Assist guarantees a high security level for Remote Assist applications, far beyond the well-known data security of VPN connections.

The most important security features of the system are:

- Any communication is encrypted and carried out via VPN connection directly from the user network to the installation network.
- Die VPNs use certificates with 1024- or 2048-bit encryption. Each VPN uses different certificates.
- The VPNs use PFS. Thereby, the data traffic cannot be decrypted.
- There is no continuous connection between the user network and that from the installation. They are completely separated by entirely independent networks. Only the Bender Remote Assist application can temporarily establish a connection between user and installation.
- Each connection is set up separately and is only valid for the requesting user to the selected installation. For access to other installations the user must request separate connections. Other users cannot use this connection. They have to request their own connection.
- All connections are logged in the Remote Assist application. Authorised users may at any time retrieve the connection protocols via the web user interface or have them sent automatically to their e-mail address.
- The rights management of the Remote Assist application ensures that a connection between user and installation is only possible if the user has the required rights.
- The rights management of the Remote Assist application in connection with the structured administration of users and installations guarantees that in all application functions any user as a principle only receives or is able to visualise information regarding the installation for which he has been given the rights by the system administrators. The user cannot obtain information from any other installation.
- The link check (monitoring of the installation availability) ensures that the Remote service can be carried out if necessary.
- Operating Bender Remote Assist in a modern and professional data centre offers a 24/7/365 usability and top availability.
- Bender Remote Assist is dedicatedly set up and operated for the user, with dedicated servers, separate IT technology and IT networks isolated from other systems.
- Connections to the system (user, installations, support) are only possible via VPN.

6.1.2 Remote access

As a part of a service package, the secure and easy remote access to installations via VPN is the core function of Bender Remote Assist.

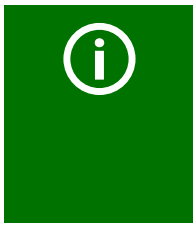
6.1.2.1 Setting up a remote access connection

The user only needs three steps to have access to the installation:

1. Log in user (refer to chapter "6.2.1 ").
2. Select installation in the window "Selection" (folder tree).
3. Click on "Connect" in the window "Installation details" and then click on "Request connection".

After a short time, the following is displayed:

- that the connection to the installation is possible for the user,
- the IP address with which the installation can be reached,
- the ports or the applications enabled for the user.



During connection set-up and during connection the system checks whether the installation is available ("Connection check"). If the installation is not available any more, connection is terminated immediately (refer to chapter " Automatic termination").
The user may not close the browser window or log himself out for the duration of the connection!

6.1.2.2 Terminating a remote access connection

Termination by the user

Click on the link "Terminate connection" displayed in the installation details in the browser window. After a short time, the connection to the installation is terminated.

Automatic termination

The connection is terminated automatically for security reasons if

- the installation is not available any more (refer to chapter "6.1.3 Link check",
- the user closes the browser window,
- the user remains inactive in the browser window for more than 480 min*,
- the connection period exceeds 480 min** (regardless of data traffic via the connection),
- during the connection the system administrator denies the user the right to connect to the installation.

* *In specific system configurations this time can be adjusted to the needs of the acquirer/user. It applies to the entire system.*

** *In specific system configurations this time can be adjusted to the needs of the acquirer/user. It applies to the entire system.*

6.1.3 Link check

The link check continuously tests the availability of the installation. In Bender Remote Assist, the system administrator can set for each installation individually whether the link check should test the installation or not. Configuration is done via the web user interface and can therefore be modified at any time.

If the installation is available,
this information is stored as a log entry in the status feature of the installation in the Remote Assist application.

If the installation is not available,
this information is also stored in the status feature but only after a configurable waiting period. The "unavailable" status is only stored for the installation if the link check has not been able to reach the installation for the entire waiting period. The waiting period is configured individually for each installation by the system administrator.
Configuration is done via the web user interface and can therefore be modified at any time. Change to "available" status is stored without any waiting period.

6.1.4 Installation status

6.1.4.1 Status values and status display

The installation status shows the user at any time

- the current availability status of the installation
- if an installation is currently being accessed.

Five statuses with the following meaning are defined:

Status value	Description
0	The availability is unknown and the installation has not been accessed yet. This status is displayed after creating an installation in the application Installations for which the link check is not activated remain in this status until first connection. In the case of installations for which the link check has been activated, the status is updated with one of the subsequent values.
1	Link check test result: installation is available. There is no access to the installation (from no user).
2	Value is only displayed in the case of (superordinate) installations (routers)! Link check test result: installation is available. At least one user accesses at least one installation or installation component in the network of the router.
3	At least one user accesses the installation, i.e. at least one user is connected to the installation. This status can only be displayed if the result of the link check test is that the installation is available. Otherwise, setting up a connection is not possible.
13	Link check test result: installation is not available.

The statuses are presented on the website using colour symbols:

Status 0:	grey symbol
Status 1:	green symbol
Status 2:	yellow-green symbol
Status 3:	yellow symbol
Status 13:	red symbol

The information is presented in tabular form.

6.1.4.2 Alert in the event of status change

Users and/or contacts in the address book can receive an alert or a notification if the installation status changes.

The main application is an immediate alert if the installation is not available any more.
A notification when the installation is being accessed can also be configured.

6.1.5 Reports

6.1.5.1 Connection reports

Connection reports consist of a tabular list that shows the history of connections to the installations.
Each report indicates:

- when the connection occurred
- who made the connection
- for how long
- to which installation did they connect
- under what firewall rules

In the report (as with all other functions of the Remote Assist application) only the installation which the user has been assigned in the rights management are listed. The user can retrieve and download connection reports interactively at any time via the web user interface for a freely selectable period of time in different file formats.

In addition, the user can determine if he wants to send connection reports to his e-mail address by activating or deactivating one or more of the following time periods:

- daily
- weekly
- monthly
- quarterly.

Connection data older than 18 months is automatically deleted from the data base once a day.

6.1.6 Alerts and notifications

6.1.6.1 Alarm groups

The configuration of alerts and notifications can be carried out by the user authorised for this function. Alarm groups can be created, modified and deleted at wish. The name is also freely editable. All or part of the installations available for an alarm group can be assigned to it.

The configuration of an alarm group contains two parts:

- the definition of the condition when an alarm should be triggered,
- the definition of the contacts to be notified when an alarm is triggered.

6.1.6.2 Alarm condition

Depending on the alarm group the following conditions can be defined:

- one or more of the installations assigned to the group switch into status 13 (not available any more).
- one or more of the installations assigned to the group switch into status 3 (the installation is being accessed).
- one or more of the installations assigned to the group switch into status 1 (installation is available (again), no access (any more)).

If a defined condition is fulfilled at one of the installations, it causes a separate alarm event in the smart Service Control Center application. This alarm event forms the basis for transmission of notifications.

6.1.6.3 Notification

The contacts that should be notified in the event of an alarm are defined in the notification area of the alarm group.

Content of a notification

Subject and text are freely selectable (when using SMS notification, the text length is limited to 160 characters). Via the web user interface, placeholders to be introduced in the text are offered, which are substituted by the specific data of the alarm event before the notification is transmitted from the Remote Assist application. Placeholders are available

- for the installation name
- for the installation description
- for the time of occurrence of the alarm event.

The notification can take place with or without escalation, depending on the system configuration.

Notification without escalation

Up to 4 contacts that should receive a notification can be defined. The following can be set individually for each contact:

- on which weekday it should be notified,
- during which time period of the day (from … to … hours) it should be notified,
- if it should be notified via e-mail and/or SMS.

The same contact can be used several times in the group of four. For each alarm event (i.e. for each installation in which the defined status change has occurred) the notification text is sent to the configured contacts (only contacts for which the time of the alarm event falls into their notification time period).

Notification with escalation
The escalation has two stages. For each stage (stage 1 and 2) 4 contacts (= stage 0) can be configured as described.

Escalation means that if none of the contacts of the preceding stage has confirmed reception of the notification to the Remote Assist application, the notifications are sent to the contacts of the subsequent stage.

The time the Remote Assist application should wait for the confirmations can be set in minutes for each stage transition of each alarm group.

The following can also be set for each alarm group:

- whether no escalation stage is used,
- whether only 1 escalation stage is used,
- whether escalation stage 1 and 2 should be used

6.1.6.4 Contacts

System users and contacts entered in the address book can be selected.

Users
The user that configures the alarm group can select from the users that he is assigned by the system administrator via the rights management of the Remote Assist application.

Address book
The address book contacts are available to all users. Editing the address book contacts is done by the system administrator.

6.1.7 Installation documentation

6.1.7.1 Documents and files

This is an installation-specific function, i.e. it is separately available for all installations.

Any file types can be uploaded for each installation to the server of the Remote Assist application. A description text can be entered for each file and the user level on which the file is visible can be selected. The size of the files to be uploaded is limited to 5 MBytes. The files available for each installation can be downloaded by the user.

6.1.7.2 Logbook

This is an installation-specific function, i.e. it is separately available for all installations. A text entry field is provided for the user. When saving the entry, user name and time stamp are completed automatically by the application and registered in the database. All entries (entry text limited) are displayed as a list, sorted by time stamp.
An additional scrollable display field shows all entries with the entire entry text.

6.2 Using the service platform

Prerequisites for using the service platform are
- correct installation of the software "OpenVPN"
- and correct setup of an OpenVPN connection!

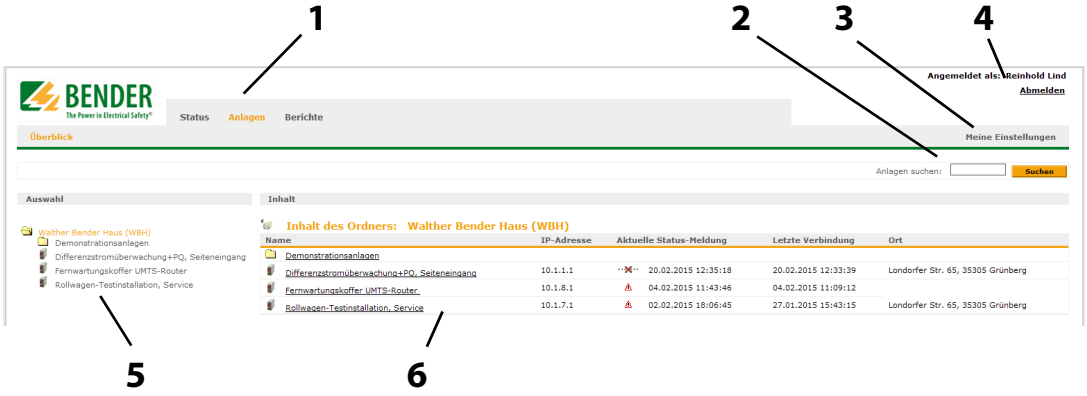
6.2.1 Logging in as a user with password

1. Start Internet browser.
2. Enter URL of the service platform: http://10.0.0.2
   The login page appears.

3. Enter user name and password.

After successfully logging in, the "Installations" window appears.

6.2.2 The "Installations" window

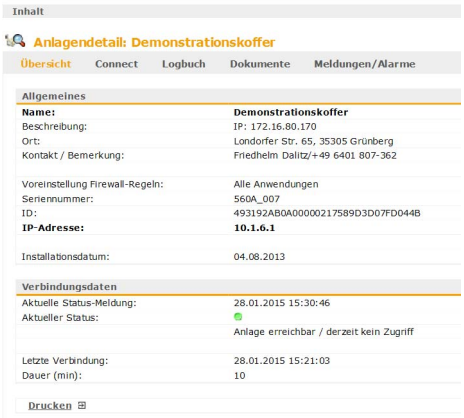


1	Status, Installations, Reports
2	Search installations
4	My settings: change user data and password
4	Log out user
5	Folder tree with subfolders
6	Folder content, installation details

6.2.2.1 Displaying installation details

1. Select installation in the folder tree.
2. Select the installation detail "Overview" in the "Content" window.

The installation master data set by the system administrator are displayed.
Click on "Print", to print out the data.



6.2.2.2 Setting up a connection

1. Select installation in the folder tree.
2. Select the installation detail "Connect" in the "Content" window.

The connection status of the installation is displayed.

- Click on "Request connection" to set up the connection to the installation.
- Click on "Terminate connection" to terminate the connection to the installation.

6.2.2.3 Using the logbook

1. Select installation in the folder tree.
2. Select the installation detail "Logbook" in the "Content" window.

The logbook of the installation is displayed. Only authorised users can create entries.

Content overview
… lists all entries line by line with

- – - Time stamp
- – - User name
- – - Text excerpt (beginning of the text)

Content
… scrollable window, which shows all entries as a list with complete text.

New entry
Used to create a new text entry (time stamp and user name are completed automatically). Click on "Save" to save the entry.

6.2.2.4 Displaying documents

1. Select installation in the folder tree.
2. Select the installation detail "Documents" in the "Content" window.

The documents assigned to the installation are displayed.

- Click on the symbol or description of a document to open it.
- Click on the symbol "  " to send the selected document via e-mail.
- Click on the symbol "  " to download the selected document to your PC.
- Click on "New entry" to assign another document.

6.2.2.5 Displaying messages/alarms

1. Select installation in the folder tree.
2. Select the installation detail "Messages/Alarms" in the "Content" window.

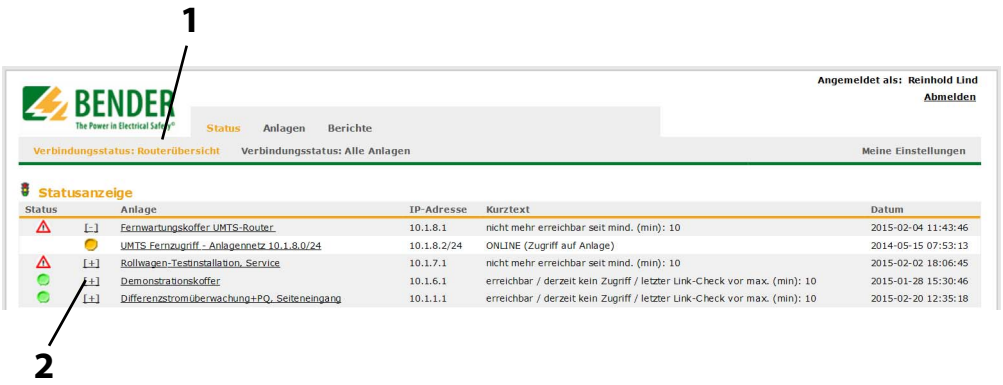
A multi-page table with messages/alarms is displayed:

Status	Indication of the status symbol, which has been switched to at the time of the message
Alarm	Alarm symbol; to differentiate between message and system message
Message text	System message: - Message text - Alarm message: - Indication of the subject line text
Point in time	Time stamp of the message

- Click on "Search for short text" to search for the text of a message.
- Click on "Export (CSV)" to entirely or partially export the table.

6.2.3 The "status" window

This window shows the connection status of the router or of the entire installation.



1	Select router overview or all installations
2	Status display: - Show sub-installations by clicking on [+] - Hide sub-installations by clicking on [-]

6.2.4 The "reports" window

The connection report lists the accesses to all installations in the selected time period: Which user has accessed which installation (name, IP address) and which port range for how long.

- Select according to time period and/or installation to display a report.
- Select a time period to receive an automatic connection report via e-mail.

6.2.5 User settings

Click on "My settings".

6.2.5.1 Displaying my settings

Your user settings and rights are displayed.

6.2.5.2 Changing my settings

1. How to change your settings
2. Enter a start page that should appear after logging in.
3. Afterwards, click on "Save".

7. Using the web user interface of the COM700RA

7.1 Basic information regarding the web user interface

7.1.1 Devices compatible with COM700RA

The COM700RA is compatible with Bender BMS devices and the PEM…. universal measuring devices. You can find a current list of devices that can be parameterised under:

http://www.bender-de.com/en > Products > Communication > COMTRAXX COM465 resp. COM460

7.1.2 Functions available via the web user interface

The device utilises an integrated web server which can be used to display data in a convenient way on any PC by means of a web browser and Silverlight™ plug-in.
In addition, it provides a Modbus TCP server which converts data of the assigned devices for a Modbus client. Also, the COM700RA contains an FTP server for file access.

- Bus overview of the assigned devices (max. 247 devices)
  - Indicating alarms and measured values.
  - Indicating the interfaces of the devices in use.
  - Indicating the harmonics in tabular form or as a chart is included for universal measuring devices. Waveform recorder and graphical representation of measured values (bar graph, phasor diagram, power triangle)
  - Parameter setting
  - Device failure monitoring
  - The "Backup/Report" function saves measured values and settings. Saved settings can be compared to current settings of the COM700RA. The saved settings can be reloaded into the COM700RA.
  - Assigning individual texts for devices, measuring points (channels) and alarms
  - Sending an e-mail notification to different user groups according to a time-controlled schedule in the event of alarms and system faults. The sender's e-mail address can be entered.
  - Indicating virtual devices. A virtual "measuring point" is obtained by logically or numerically evaluating measured values of "real" devices connected to the COM700RA.
- Management of Modbus devices
  - Adding/deleting devices to/from the bus overview.
  - Creating a template with selected measured values
- Visualisation
  - Fast and simple visualisation without any programming. Measured values or alarms can be displayed in front of a graphic (installation diagram, room plan).
  - Displaying an overview page. Jump to another view page and return to the overview page.

- From an external application (e.g. visualisation software) commands can be sent to BMS devices. The "Modbus control commands" menu provides Modbus control commands for selected BMS commands. These commands can be copied to the clipboard of the PC and then included in the programming of the external application.
- A graphical representation with the scaling of the time axis for the data logger of the COM700RA and compatible Bender devices.
- System visualisation: Displaying several gateways (COM460IP, COM700RA) on one website. Displaying common alarms of the devices. Clicking on a device being displayed will open its web user interface.
- Displaying the COM700RA operating manual.

7.2 Operating the web user interface

The web user interface is structured in the same way for all Bender gateways (CP700, COM460IP, COM700RA …). You can find detailed instructions in the manual of the CP700.

8. Data, terms, troubleshooting

8.1 Technical specifications COM700RA

CPU	Intel® Atom™ D2550 1.86 GHz
System Memory	DDR3 800/1066 SODIMM x 1.2 GB
Network (LAN)	Gigabit Ethernet, RJ-45 x 2
Serial interfaces	RS-485 x 2
Supply voltage	DC 9 . . . 30 V
Power consumption	0.5 A at 30 V
Device cooling	passive
Mounting	DIN rail mounting acc. to IEC 60715
Ambient temperature during storage and transport	-20 . . . +70 °C
Ambient temperature during operation	0 . . . +55 °C
Maximum humidity during storage	5 . . . 95 % at 40 °C
Vibration test (CFast™ Card)	5 g rms / 5 . . . 500 Hz / during operation
Shock test (CFast™ Card)	50 g peak acceleration, 11 ms duration
Electromagnetic compatibility	CE /FCC Class A
Dimensions in mm	212.15 x 78.88 x 107
Weight (net)	2.16 kg

8.2 Ordering information

Bender Remote Assist	BS99401001

8.3 Standards, approvals, certifications

CE

Quality System Certified ISO 9001

8.4 Disposal

Abide by the national regulations and laws governing the disposal of this device. Ask your supplier if you are not sure how to dispose of the old equipment.

Directive 2002/96/EG on waste electrical and electronic equipment and Directive 2002/95/EG on the restriction of certain hazardous substances in electrical and electronic equipment apply in the European Community.
In Germany, these policies are implemented through the "Electrical and Electronic Equipment Act" of 16 March 2005. According to this, the following applies:

- Electric and electronic equipment are not to be included in household waste. This is indicated by the symbol:

- Batteries and accumulators are not to be included in household waste but must be disposed of in accordance with the regulations.
- Old electrical and electronic equipment from users other than private households which was introduced to the market after 13 August 2005 must be taken back by the manufacturer and disposed of properly.

For more information on the disposal of Bender devices, refer to our homepage.

8.5 Terms used

Terms	Description
Installation	refers to a network-compatible unit, which is able to communicate with Bender Remote Assist.
Activate	enables check boxes or radio buttons displayed in the browser to execute their function.
Application	total of software programs that carry out the described functions.
Selection	clicking on a symbol/link/button displayed in the browser.
User	a person that implements the smart Service Control System.
Deactivate	check boxes or radio buttons displayed in the browser stop executing their function
Acquirer	a "person" that has legally acquired the product or the right to use the product named in the text via a purchase contract.
Main installation	in case an installation network is displayed in Bender Remote Assist, the main device indicates the router of the installation network, which constitutes the VPN terminal point of the system.
IT	information technology

Terms	Description
Network	an IT infrastructure, which enables communication to the included devices.
User	legal "person" that receives the service mentioned in the text via work and/or service contract.
Person	natural or legal person, who can enter into a contract.
PFS	Perfect Forward Secrecy. Use of session keys which are exchanged in short intervals.
Sub-installation	refers to a network-compatible unit which - is able to communicate with Bender Remote Assist, - is a part of the installation network (i.e. is in the same network), - uses the main device as a gateway.
System	total of all - related hardware and software products related or used IT infrastructure related or used services
TCP/IP	basic communication protocol for the communication in networks (LAN, Internet).
URL	Uniform Resource Locator, identifies and locates a website.
Connection	designates the ability of two network devices in a system based on TCP/IP protocol to communicate via IT infrastructure integrated in the system or used by the system.
VPN	Virtual Private Network: an encrypted and therefore secure connection (tunnel) via the Internet between a PC and a private network (e.g. company network).

8.6 Troubleshooting

8.6.1 Damage in transit

If you find transport damage on the receipt of delivery, have the damage confirmed by the delivery agent on handover. In case of doubt, please contact:

Bender GmbH & Co.KG
Londorfer Straße 65
35305 Gruenberg
Tel.: +49 6401 807-0
Fax: +49 6401 807-259

8.6.2 Malfunctions

If disturbances occur in the connected networks which might result from the use of COM700RA, please refer to this operating manual.

8.6.2.1 What should be checked?

Check whether…

- the device is supplied with the correct supply voltage
- the BMS bus cable is correctly connected and terminated (120 Ω)
- the appropriate Ethernet cable (RJ45) is connected correctly
- the BMS address is set correctly
- the IP address is set correctly or the DHCP function is activated
- the start page of the COM700RA web server can be reached via a web browser
- the current version of the Silverlight™ plug-in (at least version 5.0) is installed on the PC you are using and JavaScript is activated
- the network parameters are set correctly and at least the IP address and net mask or the DHCP function are activated.
- the sockets in the firewall of the network are activated

8.6.2.2 Where to find help?

If, after thorough reading of the technical manual and intensive fault location in your installation, you cannot clear the fault related to the Condition Monitor COM700RA, please contact our technical service department:

Tel.: **+49 6401 807-760 or 0700BENDERHELP**
Fax: **+49 6401 807-259**
E-mail: **info@bender-service.com**

INDEX

A

Alerts 25

B

Bender Remote Assist 11

C

COM700RA 12
CompactFlash card 13
Connection, preliminary considerations 14

D

Damage in transit 35
Database 12
Documents 29

H

Hardware 12
How to log in as a user 27
How to use this manual 7

I

Installation, preliminary considerations 14
Installations 27
Intended use 9

L

Link check 23
List of the BMS devices compatible with CP700 31
Logbook 28
Login page 27

M

Malfunctions 35
Menu structure of the web user interface 33
Messages/Alarms 29
Moisture 13

N

Notifications 25

O

OpenVPN 20
Ordering information 34

P

Parametrisable BMS devices, list 31
Product description 11

Q

Quick reference guide 9, 13

R

Readout of the info list 33
Remote access 22
Reports 30
Request connection 28
Rights 30
RS-485 cable 13

S

Scope of delivery 11
Service 12
Service platform 12
Software 12
Support 36
System requirements Silverlight - 14

T

Technical specifications 33
Terminate automatically 22
Terminate connection 22
Terminating resistors 13
Troubleshooting 35

U

User settings 30

V

Ventilation slots 13
VPN 11

W

Web user interface 12, 33
Work activities on electrical installations 9

BENDER
The Power in Electrical Safety©

Bender GmbH & Co. KG
P.O. Box 1161 • 35301 Gruenberg • Germany
Londorfer Straße 65 • 35305 Gruenberg • Germany
Tel.: +49 6401 807-0 • Fax: +49 6401 807-259
E-mail: info@bender.de • www.bender.de

Photos: Bender archives.

BENDER Group