Hardware and software for the Bluetooth Ethernet adapter

User manual

UM EN FL BT EPA

PHOENIX CONTACT
INSPIRING INNOVATIONS

User manual

Hardware and software for the Bluetooth Ethernet adapter

2013-04-24

Designation: UM EN FL BT EPA

Revision: 01

Order No.: —

This user manual is valid for:

Designation	Firmware version	Order No.
FL BT EPA	2.1.x	2692788
FL BT EPA AIRSET	2.1.x	2693091
FL BT EPA MP	2.2.x	2701416

Please observe the following notes

User group of this manual

The use of products described in this manual is oriented exclusively to:

- Qualified electricians or persons instructed by them, who are familiar with applicable standards and other regulations regarding electrical engineering and, in particular, the relevant safety concepts.
- Qualified application programmers and software engineers, who are familiar with the safety concepts of automation technology and applicable standards.

Explanation of symbols used and signal words

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety measures that follow this symbol to avoid possible injury or death.

There are three different categories of personal injury that are indicated with a signal word.

DANGER This indicates a hazardous situation which, if not avoided, will result in death or serious injury.

WARNING This indicates a hazardous situation which, if not avoided, could result in death or serious injury.

CAUTION This indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

This symbol together with the signal word **NOTE** and the accompanying text alert the reader to a situation which may cause damage or malfunction to the device, hardware/software, or surrounding property.

This symbol and the accompanying text provide the reader with additional information or refer to detailed sources of information.

How to contact us

Internet

Up-to-date information on Phoenix Contact products and our Terms and Conditions can be found on the Internet at:
phoenixcontact.com

Make sure you always use the latest documentation.
It can be downloaded at:
phoenixcontact.net/products

Subsidiaries

If there are any problems that cannot be solved using the documentation, please contact your Phoenix Contact subsidiary.
Subsidiary contact information is available at phoenixcontact.com.

Published by

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
GERMANY

Should you have any suggestions or recommendations for improvement of the contents and layout of our manuals, please send your comments to:
tecdoc@phoenixcontact.com

General terms and conditions of use for technical documentation

Phoenix Contact reserves the right to alter, correct, and/or improve the technical documentation and the products described in the technical documentation at its own discretion and without giving prior notice, insofar as this is reasonable for the user. The same applies to any technical changes that serve the purpose of technical progress.

The receipt of technical documentation (in particular user documentation) does not constitute any further duty on the part of Phoenix Contact to furnish information on modifications to products and/or technical documentation. You are responsible to verify the suitability and intended use of the products in your specific application, in particular with regard to observing the applicable standards and regulations. All information made available in the technical data is supplied without any accompanying guarantee, whether expressly mentioned, implied or tacitly assumed.

In general, the provisions of the current standard Terms and Conditions of Phoenix Contact apply exclusively, in particular as concerns any warranty liability.

Phoenix Contact reserves the right to register its own intellectual property rights for the product identifications of Phoenix Contact products that are used here. Registration of such intellectual property rights by third parties is prohibited.

Other product identifications may be afforded legal protection, even where they may not be indicated as such.

Table of contents

1 FL BT EPA MP

1.1 Properties

The FL BT EPA (MP) Ethernet port adapter is a high-performance, industrial Bluetooth interface for Ethernet or PROFINET-compatible devices. The FL BT EPA MP can be used as the access point to the Ethernet network for up to seven FL BT EPAs. Its typical application, however, is the point-to-point connection between two devices. This connection can be established with both variants.

A circular polarized panel antenna is permanently installed in the FL BT EPA. It enables easy establishment of stable wireless connections, especially in highly reflective environments.

The FL BT EPA MP provides an external antenna connection, enabling the use of antennas with different radiation characteristics. The option of separating the antenna from the device by means of an antenna cable also enables the wireless module to be installed in a control cabinet.

A transparent protocol is used for data transmission on Layer 2, which makes it possible to use the device in Industrial Ethernet networks such as PROFINET or Modbus/TCP.

The FL BT EPA (MP) meets the PROFINET requirements of conformance class A and the PROFIsafe profile for failsafe communication. Please also observe the relevant information on page 27.

The FL BT EPA (MP) has certified compatibility with the Bluetooth 2.1 (EDR) standard (IEEE 802.15). Bluetooth uses the FHSS method (frequency hopping spread spectrum) which is particularly resistant to radio interference, thus permitting an extremely reliable data transmission. In a limited amount of space, several Bluetooth wireless paths can be operated in parallel. Both the used ADF and black channel listing, additionally improve parallel operation with existing networks.

The range of wireless transmission greatly depends on the environment. Distances of over one kilometer can be covered under optimum conditions. In an industrial hall, typical ranges of up to 100 m can be achieved.

Figure 1-1 Front view of the FL BT EPA

1.2 Factoryline Bluetooth

Bluetooth (IEEE 802.15.1) is a standardized wireless technology, which enables extremely rugged and reliable data transmission, even in metal environments and industrial environments with high levels of interference. Bluetooth has become established as the standard for the wireless transmission of control data in automation networks. Factoryline Bluetooth is the standard-compliant optimization for industrial factory automation.

Benefits:

The use of Factoryline Bluetooth is recommended if the following requirements are to be met:

- Very reliable transmission of control data in harsh industrial environment
- A high local installation density of wireless systems
- Interference-free parallel operation with WLAN
- Protocol-transparent transmission of automation protocols (e.g., PROFINET, EtherNet/IP)
- Optimization for PROFINET operation (PN prioritization, PTCP filter, etc.)
- Ranges of up to 100 m indoors and several hundred meters outdoors (strongly depends on environmental conditions)

1.3 Approvals

The FL BT EPA (MP) is a Bluetooth wireless module used for the wireless connection of Ethernet-compatible devices to one another or to a LAN. The device uses the international license-free WLAN standard which is free of charge and operates in the 2.4 GHz ISM band. This enables worldwide use.

The device meets all the requirements of R&TTE directive 1999/5/EC (Europe).

For European approvals, please refer to the CE declaration of conformity at phoenixcontact.com.

In addition, the following approvals have been carried out and passed:

– FCC/CFR 47, Part 15 (USA)
– RSS 210 (Canada)

Depending on the maximum possible transmission power, device operation must be approved or registered in some countries. In addition, there may be a usage restriction on the transmission power for indoor and outdoor use.

The FL BT EPA (MP) has a maximum transmission power of 10 mW (10 dBm) and corresponds to R&TTE device class 2. Please refer to the list of country approvals to see for which countries the operation of this device has been approved (please observe the corresponding usage restrictions*):

An up-to-date list of the country registrations can be found in the e-shop at phoenixcontact.com. Approvals for other countries are available on request.

France: a maximum transmission power of 10 mW (10 dBm) is permitted outside buildings. The transmission power must be adapted in the web-based management by taking into account the antenna data.

1.4 Firmware versions and their functions

In addition to the standard Bluetooth functions, the firmware functions as of version 2.1.x provide a dynamic web interface and additional PROFINET optimizations. They can be used with hardware version 2.3 or later.

1.5 FCC information

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

– – Reorient or relocate the receiving antenna.

– – Increase the separation between the equipment and receiver.
– – Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
– – Consult the dealer or an experienced radio/TV technician for help.

To comply with FCC part 15 rules in the United States, the system must be professionally installed to ensure compliance with the Part 15 certification. It is the responsibility of the operator and professional installer to ensure that only certified systems are deployed in the United States. The use of the system in any other combination (such as co-located antennas transmitting the same information) is expressly for bidden.

FCC Caution

Any changes or modifications not expressly approved by the party responsible for compliance could void the user´s authority to operate this equipment.

This 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 and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

IC Statement

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B conforme á la norme NMB-003 du Canada.

This device complies with Industry Canada license-exempt RSS standard(s). Operation this 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.

Le présent appareil est conforme aux CNR d`Industrie Canada applicables aux appareils radio exempts de licence. L`exploitation est autorisèe aux deux conditions suivantes: (1) l`appareil ne doit pas produire de brouillage, et (2) l`utilisateur de l`appareil doit accepter tout brouillage adioèlectrique subi, mème si le brouillage est susceptible d`en compromettre le fonctionnement.

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and it´s gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

This radio transmitter (identify the device by certification number, or model number if Category II) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

The device could automatically discontinue transmission in case of absence of information to transmit, or operational failure. Note that this is not intended to prohibit transmission of control or signaling information or the use of repetitive codes where required by the technology.

IMPORTANT NOTE:

IC Radiation Exposure Statement:

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between radiator & your body.

This module is intended for OEM integrator. The OEM integrator is still responsible for the IC compliance requirement of the product, which integrates this module.

20cm minimum distance has to be able to be maintained between the antenna and the users for the host this module is integrated into. Under such configuration, the IC RSS-102 radiation exposure limits set forth for a population/uncontrolled environment can be satisfied.

Any changes or modifications not expressly approved by the manufacturer could void the users authority to operate this equipment.

1.6 Mounting the FL BT EPA (MP)

A minimum distance of 50 cm between modules must be observed when mounting the FL BT EPA (MP).

Make sure that the antenna is not located directly in front of a metal surface. Otherwise, the radio characteristics of the antenna may be considerably affected. Observe a minimum distance of 20 cm between devices and personnel.

1.6.1 Mounting the FL BT EPA (MP) on a level surface

Mount the FL BT EPA (MP) on a level mounting surface and secure it with two screws (e.g., 84-M3 X 35-8.8 cylinder head screws). For the required drill hole spacing, please refer to Figure 1-2 on page 6.

1.6.1.1 Drill hole template and housing dimensions

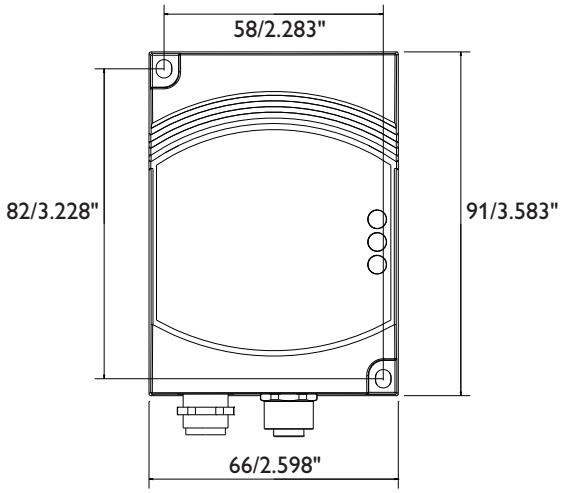


Figure 1-2 Housing dimensions and drill hole spacing for the device in millimeters (inches)

1.6.2 DIN rail mounting

The FL EPA RMS mounting kit (2701133) is available as an accessory for mounting the device on a 35 mm DIN rail.

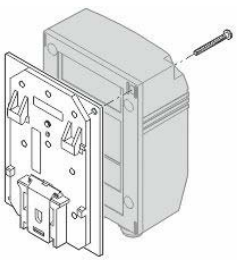


Figure 1-3 Fixing the EPA to the mounting kit for the DIN rail

- Use the two screws provided to fix the EPA to the base plate.
- Place the EPA with the adapter on the top edge of the DIN rail.
- Push the EPA towards the DIN rail until it snaps into place.
- For releasing the adapter from the DIN rail, pull the latch downwards using a screwdriver and simultaneously remove the EPA from the DIN rail.

1.6.3 Wall or mast mounting

The FL EPA WMS (2701134) mounting kit can be used for EPA wall or mast mounting.

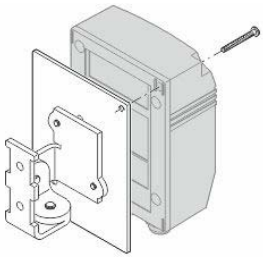


Figure 1-4 Fixing the EPA to the mounting kit for wall/mast mounting

- Use the two screws provided to fix the EPA to the base plate.
- The two 4.5 mm bore holes can be used for mounting. Two steel clamps are provided for mounting the EPA to a mast (25 - 85 mm).

NOTE: Observe the permitted operating temperatures of the EPA when using it outdoors. The device is suitable for installation in protected outdoor areas (e.g., under a porch). Direct sunlight may lead to overheating and permanent damage of the device.

1.7 FL BT EPA MP installation/interfaces

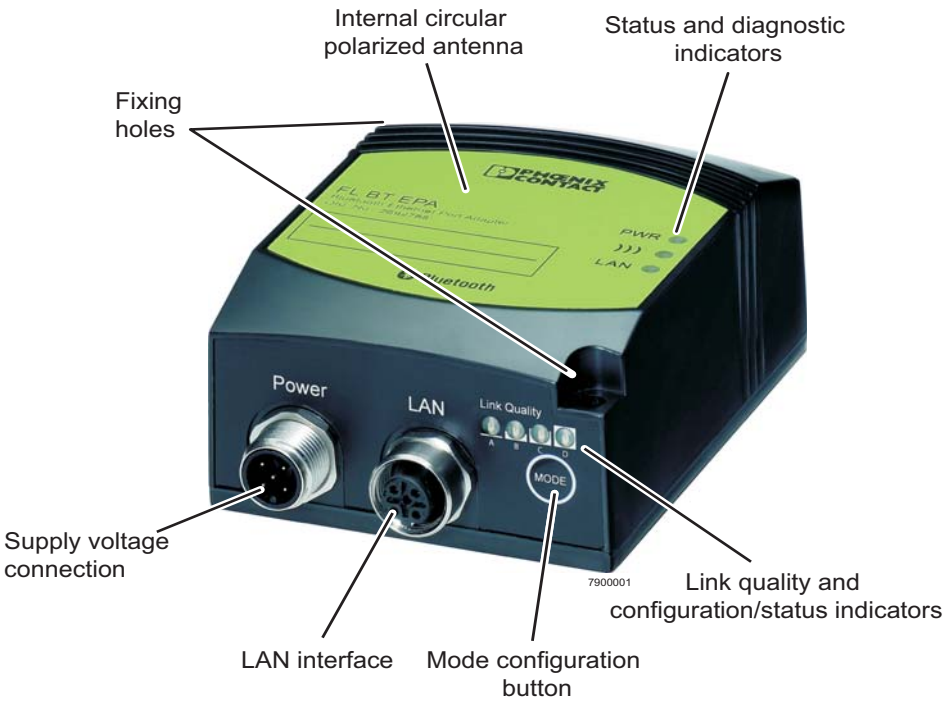


Figure 1-5 View and interfaces of the FL BT EPA MP

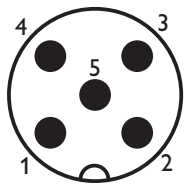
– Fixing holes
  These holes can be used to fix the BTAP on a level mounting surface with two screws (e.g., 84-M3 X 30-8.8 cylinder head screws) (for drill hole spacing, see Figure 1-2 on page 6).
– Antenna
  The device is supplied with an **internal** circular polarized 5 dB panel antenna. The internal antenna cannot be replaced.
– Supply voltage connection
  The supply voltage is connected via the 5-pos. M12 socket (plug on the device).
– Network connection
  Copper interface in M12 format (socket on the device) with 10/100 Mbps with auto negotiation.
– Status and diagnostic indicators
  The LEDs indicate the status of the Ethernet and Bluetooth interfaces or act as configuration indicators.

1.7.1 Electrical connection

The supply voltage and the trigger signal are connected via the 5-pos. M12 plug (A-coded) labeled “Power” (see Figure 1-5 on page 8).

1.7.1.1 Pin assignment for the connection of the trigger input DI and the supply voltage

Pin 1 Vin + (9 - 30 V DC)
Pin 2 External trigger ground
Pin 3 Vin GND (0 V)
Pin 4 External trigger + (9 - 30 V DC), responds to a rising edge
Pin 5 n.c.



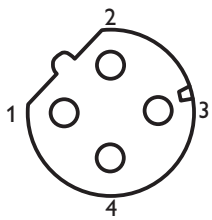
A-coded Male M12

Figure 1-6 View of the supply voltage connection - plug on the device (contact side, not solder side)

Make sure that the trigger input is not permanently connected with VIN +.

1.7.1.2 Assignment of the LAN socket

Pin 1 Transmit +
Pin 2 Receive +
Pin 3 Transmit -
Pin 4 Receive -



D-coded Female M12

Figure 1-7 View of the network connection - socket on the device (contact side, not solder side)

1.7.2 Status and diagnostic indicators

Three LEDs are located on the top of the device, which indicate different states.

Figure 1-8 LEDs on the top of the device

On the bottom of the device, there are four LEDs which display alternative information depending on the operating mode.

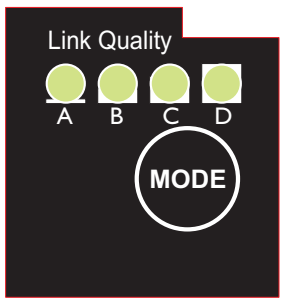


Figure 1-9 LEDs on the bottom of the device

The MODE button is used for configuration. Please observe its function in the user manual. LEDs “A” to “D” are used to indicate the status during configuration (see Section “Configuration using the MODE button” on page 20).

Des.	Color	Status	Meaning
PWR	Green	ON	Supply voltage present
		Flashing	Supply voltage too low
		OFF	Supply voltage not present
)))	Blue/ purple/ red	Lights up blue	A Bluetooth connection has been established
		Purple	Attempt to establish a connection to another Bluetooth device
		Flashing blue	Data transmission
		Red	Error
		OFF	Device waits for connection requests

Des.	Color	Status	Meaning
LAN	Yellow	ON	Ethernet link present
		Flashing	Ethernet communication active
		OFF	No Ethernet connection
Link Quality	Green	ON	A: poor link quality A and B: sufficient link quality A, B, and C: good link quality A, B, C, and D: excellent link quality

2 Startup and configuration

2.1 Device configuration options

There are different ways of configuring the EPAs for operation:

MODE button

Typical operating modes, such as direct connection of two EPAs as a “wireless Ethernet cable”, can be directly selected via the MODE button on the EPA without the need for a PC. A detailed description can be found in Section 2.1.1 on page 20.

Web-based management (WBM)

To use all the options, the device has a web-based management, which provides a graphical user interface via a web browser. This means that the current operating state can simply be displayed without the use of special software or the device can be configured using a password.

For parameter description, please refer to the parameter list in Section 2.4 on page 30.

AT commands

All the EPA parameters can be modified or transmitted to the EPA in an automated manner, for example from a program of a controller. For development or testing purposes, AT commands can also be transmitted to the EPA via the WBM or directly via any web browser.

For the AT command reference, please refer to the Phoenix Contact download center (phoenixcontact.com). The procedure is described on page 28.

SSC script

If easy, quick, and reliable startup of numerous devices is required, even complex configurations can be stored in the form of an SSC script and transmitted to the EPA via the Windows Scripting Host (WSH) from any Windows PC without the need for special software.

For detailed instructions and example scripts, please refer to Section 2.5 on page 37.

SNMP

The Simple Network Management Protocol (SNMP) is primarily used to configure and maintain complex networks. It enables central access to the device parameters independent of the manufacturer. The EPA provides the corresponding support.

For a detailed description, please refer to 3 on page 41.

2.1.1 Configuration using the MODE button

Figure 2-1 MODE button on the bottom of the FL WLAN EPA - Above the MODE button are LEDs “A” to “D” for configuration indication

General sequence:

- Connect the module to the power supply.
- **Within 5 seconds** of switching on the supply voltage, briefly press the MODE button to access configuration mode.
- Select the desired operating mode by repeatedly pressing the MODE button until the corresponding LED combination lights up. Once you have scrolled through all the LED combinations (operating modes), the selection automatically starts again from the beginning.
- After selecting the desired operating mode, exit the configuration by pressing the MODE button (> 2 seconds) until the LEDs flash or go out (upon reset or when exiting configuration mode).

If the module has been previously configured, we recommend restoring the device's default settings before configuring the device via the MODE button. This action is also performed via the MODE button.

If the MODE button is not pressed in the active configuration mode for an extended period, the configuration mode is automatically exited and the EPA is started in its previous setting.

Table 2-1 Permissible LED combinations when starting up via MODE button

Mode	Operating mode	Configuration setting	LEDs	A	B	C	D
1	PANU	**Activate DHCP server** The EPA operates as DHCP server and, for example, assigns address 10.0.0.1 to a computer which is connected for configuration purposes via DHCP. Not to be used for operation in a network.	A	●			
2	PANU	Reset the device to the **default settings.**	B		●		
3	PANU	Reset the **IP parameters** to the default settings (10.0.0.100). Other settings are not modified.	A+B	●	●		

Table 2-1 Permissible LED combinations when starting up via MODE button

Mode	Operating mode	Configuration setting	LEDs	A	B	C	D
4	PANU	**EPA-to-EPA bridge: wait for configuration** Step 1 for establishing a direct connection (PANU-PANU) between two EPAs. As long as the LED flashes, the module waits for a connection request. After connection establishment the module accepts IP address 10.0.0.99. Another address can be assigned via DHCP.	C			●	
5	PANU	**EPA-to-EPA bridge: connection establishment** Step 2 for establishing a direct connection (PANU-PANU) between two EPAs. The module initializes connection to a module in mode 4 - “Wait”. After connection establishment the module accepts IP address 10.0.0.100. Another address can be assigned via DHCP.	A+C	●		●	
6	PANU	**EPA-to-EPA bridge with PROFINET optimization:** Connection establishment Step 2 for establishing a direct connection (PANU-PANU) between two EPAs. The module initializes connection to a module in mode 4 - “Wait”. SafetyBridge transmission requires the settings page of the web interface to be switched off. After connection establishment the module accepts IP address 10.0.0.100. Another address can be assigned via DHCP.	B+C		●	●	
7	PANU	**Connection to an FL BT EPA MP in access point mode:** Connection establishment Step 2 for establishing a connection to an “access point” (NAP) in state “10 - Wait for client”. After connection establishment the module accepts IP address 10.0.0.100. Another address can be assigned via DHCP.	A+B+C	●	●	●	
8	PANU	**EPA-to-EPA bridge: connection establishment with EDR** Step 2 for establishing a direct connection (PANU-PANU) between two EPAs. The module initializes connection to a module in mode 4 - “Wait”. This mode allows for higher data rates. However, it is dependent on a better wireless connection. After connection establishment the module accepts IP address 10.0.0.100. Another address can be assigned via DHCP.	D				●

Table 2-1 Permissible LED combinations when starting up via MODE button

Mode	Operating mode	Configuration setting	LEDs	A	B	C	D
9	PANU	**EPA-to-EPA bridge: connection establishment with EDR and PROFINET optimization** Step 2 for establishing a direct connection (PANU-PANU) between two EPAs. The module initializes connection to a module in mode 4 - “Wait”. This mode allows for higher data rates. However, it is dependent on a better wireless connection. SafetyBridge transmission requires the settings page of the web interface to be switched off. After connection establishment the module accepts IP address 10.0.0.100. Another address can be assigned via DHCP.	A+D	●			●
10	NAP	Personal Area Network (PAN): “Wait for client login” Step 1 for establishing a multipoint connection (PAN). As long as the LED flashes, the module waits for a connection request (from an EPA in mode 7). To register additional devices, this mode can be selected again. After connection establishment the module accepts IP address 10.0.0.99. Another address can be assigned via DHCP.	B+D		●		●

● = LED ON

2.1.2 Configuration example

2.1.2.1 Example 1: Reset EPA module to default settings.

- Switch on the EPA module and press the MODE button after power up to change to configuration mode. The “A” LED will light up now.
- Then press the MODE button once until the “B” LED lights up. Once the mode has been selected, press the MODE button again and hold it down for at least two seconds until the corresponding mode LED goes out. The EPA module is now reset to its default settings.

2.2 Delivery state/default settings

By default upon delivery or after the system is reset to the default settings, the following functions and properties are available:

– The password for configuration in the WBM is “admin”.
– The WLAN AP is supplied with the following IP parameters:
IP address: 10.0.0.100
Subnet mask: 255.255.0.0
Gateway: 10.0.0.100
– DHCP is not activated as the addressing mechanism.

2.3 Web-based management

To configure the EPA via the graphical user interface of the web-based management, enter the EPA's IP address in the address line of your web browser.

By default upon delivery or after the system is reset to the default settings, the address is:

http://10.0.0.100

Then the information page of the EPA opens:

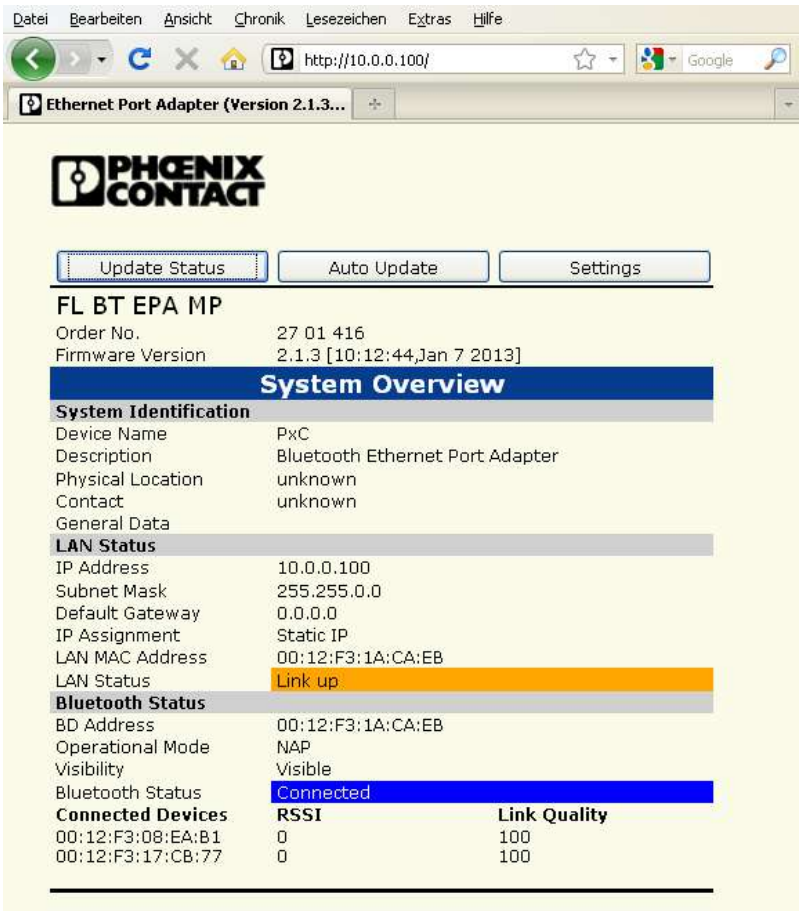


Figure 2-2 “System Overview” web page

This page displays current information on the operating state of the EPA. However, the settings cannot be changed here.

Pressing the “Update Status” button updates the values once; pressing the “Auto Update” button triggers an automatic update every second.

In order to make full use of functionality, the browser must support HTML 5.

For example, the following browsers are supported:

– Google Chrome - Version 10 or later
– Apple Safari - Version 5 or later
– Mozilla Firefox - Version 3.6 or later
– Microsoft Internet Explorer - Version 9 or later
– Opera - Version 10.1 or later

The automatic update function causes an additional system load which might reduce the performance of the actual communication.

For a detailed description of the parameters, please refer to the overview at the end of this section.

Pressing the “Settings” button changes to the configuration view. The configuration page will only be displayed after entering the password.

Figure 2-3 “Login” screen

- Enter the password and confirm by clicking “Enter” or the “Login” button.

The default login password is “admin”. For reasons of security, it is essential to assign a secure and secret password prior to live operation.

If the operating mode (PROFIsafe) has been selected via the MODE button, the information page is displayed but the configuration cannot be accessed. This prevents accidental changing of parameters that might be relevant for the operation of devices with safety functions. In this case, the configuration can only be accessed by resetting the EPA using the MODE button.

The configuration page is based on the operation of the device. Only the options for the current configuration are shown. We therefore recommend to work through the page from top to bottom.

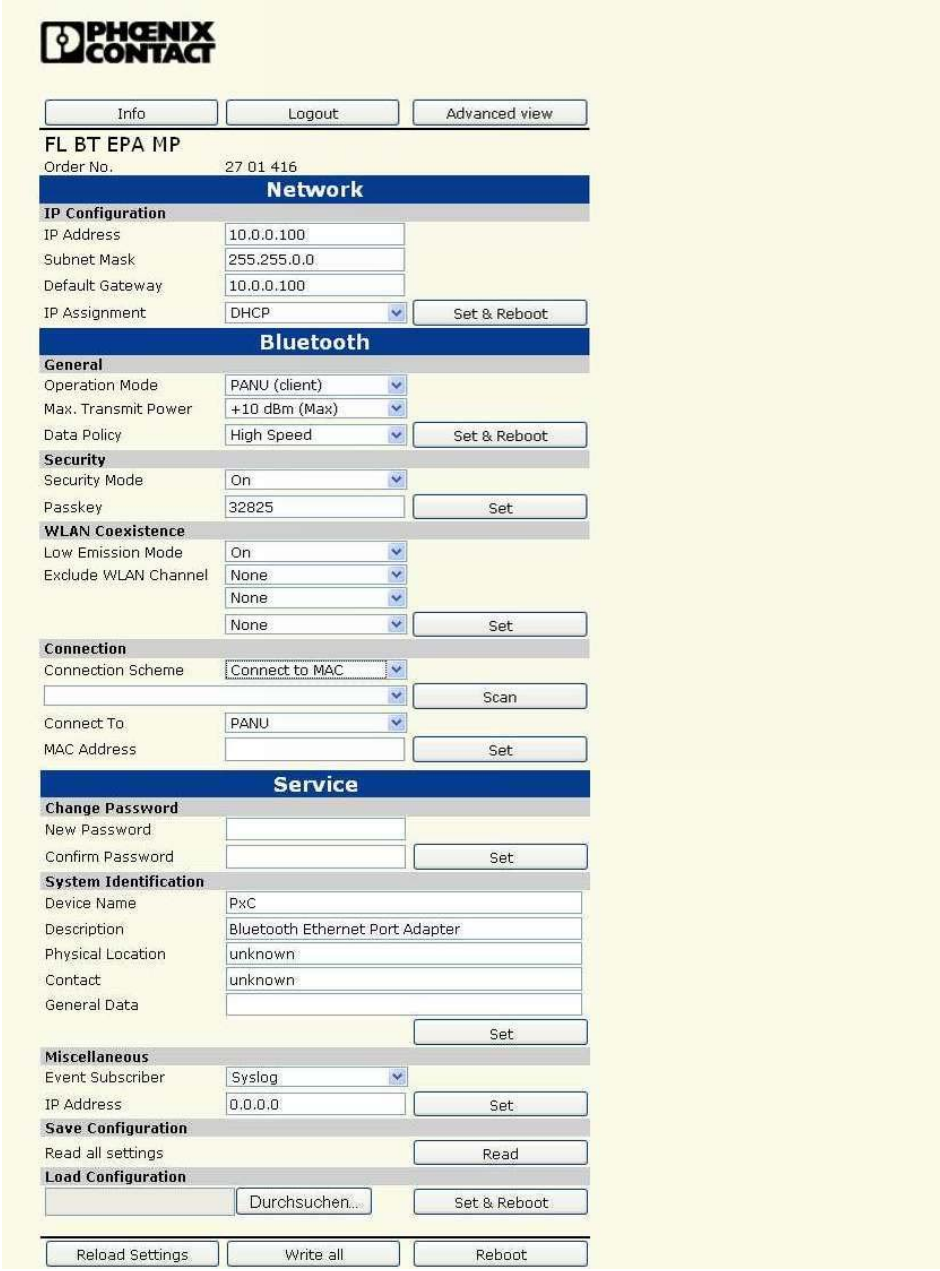


Figure 2-4 Configuration menu

All the sections contain a “Set” or “Set & Reboot” button. The parameters of each section are only transferred to the EPA and stored permanently with a click on the relevant button.

2.3.1 Configuration example

Connecting a device of type FL BT EPA to an FL BT EPA MP:

The following information is required:

– EPA IP adress: 192.168.0.90 (static)
– Subnet mask: 255.255.255.0

Application: connection of Bluetooth client (PANU) to Bluetooth access point (NAP)

– Bluetooth name: “LaneA”
– Encryption activated, key: “MyKey4LaneA”

How to proceed:

Setting up the access point (NAP, for FL BT EPA MP only)

1. Enter the new IP address, subnet mask (and gateway, if applicable) of the EPA. Change the type of address assignment (“IP Assignment”) from “DHCP” to “Static”. Apply the settings with “Set & Reboot”. (At this point, the WBM restarts with the new IP address.)
2. Change the operating mode to “NAP” and restart the device with “Set & Reboot”.
3. In the “Security” section, change the passkey to “MyKey4LaneA”. Transfer the entry with “Set”.
4. In the “Connection” section, change the “Connection Scheme” to “Wait (Name)”. Enter the Bluetooth name “LaneA” in the “Name” field. Transfer the entry with “Connect”.
5. Assign a secret and secure password for the WBM. To avoid write errors the password must be entered twice, in the “New Password” and “Confirm Password” fields. Apply the new password with “Set”. From now on, the configuration page can only be accessed using this password. If the password is lost, the device can be reset to the default settings using the MODE button. However, the entire configuration will also be lost.

Optimizations (e.g., for PROFINET):

– Under “Bluetooth – General, the “Data Policy” entry should be set to “Short Delay”. This ensures that only DM 3 packets are used on the wireless side that are optimally tailored to the length of standard PROFINET packets.

The following parameters can be used provided that the client-access point connections are not to be changed during operation (static network):

– In the “Bluetooth Connection” section, the number of clients can be entered. This will lead to an increased performance, because the access point does not reserve (radio) time to connect additional clients.
– The “Start Of Communication” parameter can be changed to “After all clients completed”. In this case, there will be no data transmission until the number of clients specified above has been connected. By concentrating on connection establishment, the clients are registered as quickly and reliably as possible. Make sure you specify the correct number of clients.

Setting up the client (FL BT EPA and FL BT EPA MP in PANU mode)

1. Enter the new IP address, subnet mask (and gateway, if applicable) of the EPA. Change the type of address assignment (“IP Assignment”) from “DHCP” to “Static”. Apply the settings with “Set & Reboot”. (At this point, the WBM restarts with the new IP address.)
2. In the “Security” section, change the passkey to “MyKey4LaneA”. Transfer the entry with “Set”.
3. In the “Connection” section, change the “Connection Scheme” to “Connect to Name (Fast)”. Enter the Bluetooth name “LaneA” in the “Name” field. Transfer the entry with “Set”.

Optimizations (e.g., for PROFINET):

– Under “Bluetooth – General, the “Data Policy” entry should be set to “Short Delay”. This ensures that only DM 3 packets are used on the wireless side that are optimally tailored to the length of standard PROFINET packets.

Now configuration is complete.

The settings that are not transferred to the EPA via “Set” are neither activated nor stored. In any case, complete every section where changes have been made by clicking the “Set” button.

Advanced view

When clicking on the “Advanced view” button, additional elements are shown on the right side of the window.

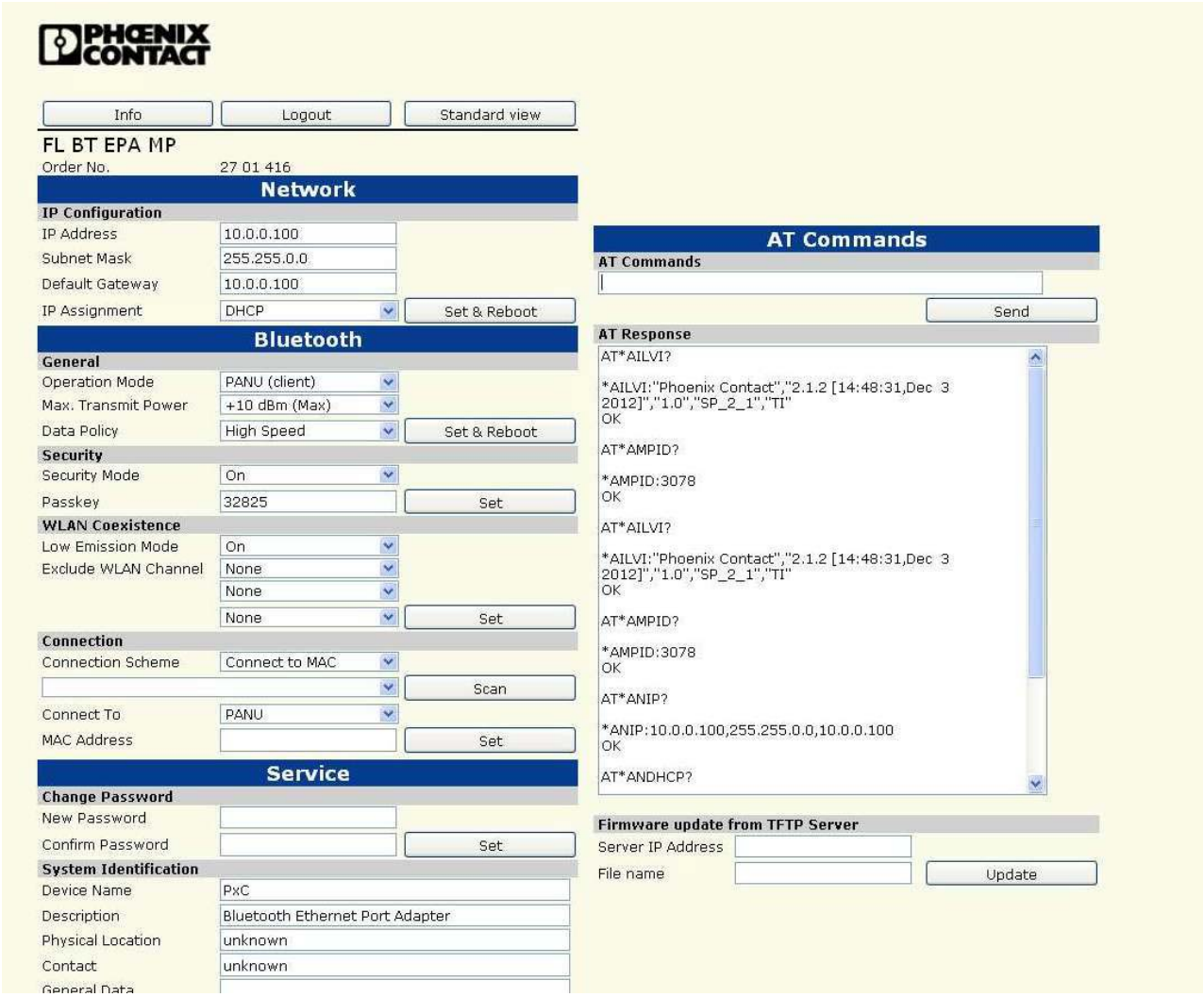


Figure 2-5 “Advanced” menu

Two additional functions are available for selection:

– Display and execution of AT commands
– Firmware update

AT commands

All the important configuration options are directly available on the graphical interface. For special parameter combinations, operating elements are available here to send AT commands to the EPA or to display return values.

To do so, enter the command in the “AT Commands” entry field and click on the “Send” button. The result is shown in the “AT Response” text field.

For a complete AT command reference, please refer to download.phoenixcontact.com

The “AT Response” window also shows the commands sent via the graphical interface. This overview can simply be used as a basis for automatic configurations from control programs or SSC scripts.

Firmware update

The “Firmware update from TFTP Server” section can be used to transmit new firmware versions.

Enter the IP address of the TFTP server and the name of the firmware file in the text fields and click on the “Update” button. The firmware is then transmitted to the EPA and installed. Most of the settings are retained.

For firmware updates, a TFTP server program is required. A wide range of products is available on the Internet. For an example instruction along with the current firmware version, please refer to download.phoenixcontact.com.

During firmware update, the autocrossing function is not available. Therefore, use a switch or a crossed cable.

2.4 Parameter list for the configuration

Table 2-2 Parameter list for Info page

Designation	Description
Update Status	Update display.
Auto Update	Update display automatically. The additional data load may affect the actual communication.
Settings	Change to configuration page.
Order No.	Order number of the device
Firmware Version	Installed firmware version. You may find a more recent version in the download area of this article at phoenixcontact.com.
System overview	
System identification	
Device Name	Device name (information only), e.g., used for SNMP.
Description	Device description (information only), e.g., used for SNMP.
Physical Location	Device location (information only), e.g., used for SNMP.
Contact	Responsible contact (information only), e.g., used for SNMP.
General Data	General data (information only), e.g., used for SNMP.
LAN Status	
IP Address	Layer 3 network address (IP) of the EPA, default: 192.168.0.254
Subnet Mask	Filter mask for IP addresses, default: 255.255.0.0
Default Gateway	IP address of the transition point to other network segments. Not required for communication within the own address area.
IP Assignment	**Type of address assignment** – Static + DHCP Relay (default): static IP address, assignment via the entry field on the “Settings” page. Its standard value is: 192.168.0.254. Devices connected via the LAN side can place DHCP requests in the network. – DHCP: IP address of the EPA is retrieved from an active DHCP server in the network. In the case that address assignment fails, the EPA uses the address set in the WBM. – Static & DHCP Server: the EPA itself uses the address permanently set, and operates as the DHCP server for other devices on the LAN side (start address: 192.168.0.1).
LAN MAC Address	Layer 2 device address (MAC) of the LAN connection (permanently assigned)

Table 2-2 Parameter list for Info page [...]

Designation	Description
LAN Status	Current connection status of the LAN connection Link up - connected. This indication corresponds to the LAN LED on the device.
Bluetooth status	
BD Address	Layer 2 device address (MAC) of the Bluetooth wireless module (permanently assigned)
Operational Mode	Operating mode PANU: client within a personal area network (PAN), can also be used for point-to-point connections. NAP: network access point (“master” in a PAN), up to seven connections can be managed.
Visibility	Visibility In order to establish connection on the basis of a network name, Bluetooth devices will send an inquiry scan. The “Visibility” property determines whether a device responds to an inquiry scan, thus being “visible” to other devices. This property does not have any influence on connection requests based on the MAC address.
Bluetooth Status	Indicates whether there is a Bluetooth connection. The color corresponds to that of the LAN LED on the device. Disconnected (white background): not connected, device passive Connecting (violet background): not connected, device searches for a partner (active) Connected (blue background): device connected
Connected Devices	List of connected devices, can be identified via the MAC address of the partner RSSI: signal strength, “0” under optimum conditions, borderline if below “-20” Link Quality: percentage, “100” under optimum conditions
Login	
Login to gain access	
Password	Entry field for the password of the configuration page (default: admin)
Login	Log in for configuration If PROFINET optimization is active, access to the configuration page is disabled.
Cancel	Cancel login, return to Info page.
Settings	
Settings	

Table 2-2 Parameter list for Info page [...]

Designation	Description
Info	Return to Info page. The user remains logged in.
Logout	Return to Info page. The user is logged off.
Advanced view	Extend view by AT commands and the firmware update option.
Network	
IP configuration	
IP Address	Enter layer 3 network address (IP) of the EPA. The address must be unique in order to address the WBM during operation.
Subnet Mask	Enter filter mask for IP addresses, default: 255.255.0.0
Default Gateway	Enter IP address of the transition point to other network segments, default: 10.0.0.100 Not required for communication within the address area.
IP Assignment	**Select the type of address assignment** – Static: permanent assignment via the “IP Address” entry field (default). The standard value is 10.0.0.100. – DHCP: address is retrieved from an active DHCP server in the network. In the case that address assignment fails, the EPA uses the address set in the “IP Address” field. – Static & DHCP Server: the EPA itself uses the address permanently set, and operates as the DHCP server for other devices on the LAN side (start address 10.0.0.1).
Bluetooth	
General	
Operating Mode	Operating mode of the device PANU: client within a personal area network (PAN), can also be used for point-to-point connections. NAP: network access point (“master” in a PAN), up to seven connections can be managed.
Max. Transmit Power	Selection of the maximum transmission power (at the output of the transmission level, the antenna gain of approx. 5 dBi must be added in the case of an internal antenna) Note: Bluetooth automatically reduces the actual transmission power to the level required for the current connection. Manually reducing the transmission power is only recommended for range limitation.

Table 2-2 Parameter list for Info page [...]

Designation	Description
Data Policy	Optimizing the data transmission method High Speed (default): All packet sizes (DM and DH) are selected automatically. The system automatically selects the most suitable packet size for the Ethernet packet. Short Delay: All DM packet sizes and QoS prioritizing are used, resulting in the lowest possible latency. High Range: Only DM1 packets can be used for the system. Transmission will be slower, however more robust and particularly in the event of long distances and/or demanding environments more advantageous. EDR: Optimum transmission standard, as long as the BT2.1+EDR standard is supported by both sides.
Security	
Security Mode	Activate/deactivate security (encryption and authentication): ON (default): encryption and authentication must be used. (GAP security mode 3 with encryption) OFF: No additional security mechanisms. Each device can log in without having to enter a passkey. (GAP security mode 1 without encryption)
Passkey	Key to be entered for authentication during connection establishment. Make sure you choose a unique and secure key.
WLAN coexistence	
Low Emission Mode	**Activate low emission mode** – OFF (default): LEM 0 - The behavior corresponds to that of the Bluetooth standard. Enables operation with standard-compliant Bluetooth devices. – ON: LEM 3 - The device has less impact on the wireless channel during connection establishment. This mode is particularly recommended for parallel operation with WLAN networks. Note: Both communication partners must operate in the same LEM mode. Otherwise, connection establishment can take a very long time.

Table 2-2 Parameter list for Info page [...]

Designation	Description
Exclude WLAN Channels	Select WLAN channels that should not be used by the Bluetooth system. (WLAN black channel list) The WLAN channels selected here will be excluded in the BT jump sequence. A maximum of three WLAN channels can be hidden without restricting the function of the Bluetooth system. By excluding WLAN channels, the available bandwidth will be reduced and thus the number of Bluetooth systems that can be operated parallel to each other. WLAN channels should only be hidden if they are actually required for high-availability WLAN systems.
Connection	
Connection Scheme in “PANU” operating mode (client)	Connect to MAC: Based on the MAC address, a direct connection is established to another device. The MAC address can either be entered directly in the “MAC address” field or taken from a “scan”. (Devices in “Invisible” mode cannot be displayed.) Connect to Name (Best RSSI): Searches for a connection to a Bluetooth device with the corresponding name. In this setting, all responses to the connection request will be waited for and the connection will then be established to the partner with the highest receive field strength. Connect to Name (Fast): Scans for partners and establishes a connection to the first device responding with a matching name. This mode is faster than “Best RSSI”, however, it does not always ensure the optimum connection. Connect to Name (P2P only): Scans for a partner and attempts to establish a connection that is based on the first response. Should this partner not belong to the corresponding network (i.e., the name does not match) the attempt at connection establishment will be aborted. Using this mode, connections are established very quickly. However, it can only be used if there are no visible devices of other networks (names). Therefore, only use this mode for dynamic, but clear point-to-point connections. In order to establish connection on the basis of a network name, the partner must be “visible”, i.e., it must respond to an inquiry scan. The EPAs are “visible” up to the point where the maximum number of connections is reached. Thereafter, the devices will no longer respond to a scan. For all Bluetooth networks, it is in general not possible to ensure a maximum time limit for changing from one wireless cell to another (roaming). The roaming times will increase with increasing Bluetooth network utilization.

Table 2-2 Parameter list for Info page [...]

Designation	Description
Connection Scheme in “NAP” operating mode (access point)	Wait (MAC): Based on the MAC address, other devices can connect to the access point very quickly in this operating mode. Wait (Name): The access point waits for connection requests based on the network name. Bluetooth clients are able to dynamically connect to different access points. In this case, enter the Bluetooth name (“network name”) in the “Local Name” field. In addition, this mode considerably facilitates device replacement since the configuration of clients must not be changed. In order to establish connection on the basis of a network name, the partner must be “visible”, i.e., it must respond to a scan. The EPAs are “visible” up to the point where the maximum number of connections is reached. Thereafter, the devices will no longer respond to a scan. For all Bluetooth networks, it is in general not possible to ensure a maximum time limit for changing from one wireless cell to another (roaming). The roaming times will increase with increasing Bluetooth network utilization.
Connect to	Select the operating mode of the partner to which a connection should be established. NAP: The partner is in the NAP (“Access point”) mode. PANU: The partner is in the PANU (“Client”) mode.
SCAN	Search for available Bluetooth devices.
Tabelle	After “scan” the available Bluetooth devices are displayed with MAC address, network name and RSSI value (receive field strength). Select an entry. The MAC address and network name are shown in the corresponding fields.
Name / Local Name	Bluetooth network name (used for connection establishment) Only those characters of the network name that have been entered in the “active” device will be compared. The network name of the “passive” device (i.e., the device waiting for a connection) can be longer. E.g.: (active -> passive connection) TestName -> TestName yes Test -> TestName yes TestName -> Test no

Table 2-2 Parameter list for Info page [...]

Designation	Description
Max. No of Clients	Enter maximum number of connections. When the actual number of (possible) connections is indicated, the access point is not required to reserve time slots for additional connection requests. System performance will be improved.
Start of Communication	Immediately: LAN communication is started directly after connection establishment. Ensure that you choose this option if connections may dynamically change during operation. After all clients completed: LAN communication will only start when the number specified for “Max. no. of Clients” is connected. The wireless path remains unused at this stage, connection establishment will accelerate. Only select this option if the devices cannot be changed during operation.
Service	
Change password	
Password	Enter new password for the WBM. Make sure to replace the standard password by a secret and secure password for security reasons.
Retype Password	Re-enter password to avoid typing errors.
System identification	
Device Name	Enter device name (display for SNMP or on Info page, for example).
Description	Enter device description (display for SNMP or on Info page, for example).
Physical Location	Enter installation location (display for SNMP or on Info page, for example).
Device Contact	Enter contact (display for SNMP or on Info page, for example).
General Data	Enter additional descriptive text (display for SNMP or on Info page, for example).
Miscellaneous	
Event Subscriber	Activate documentation of system events via TCP or Syslog.
IP Address	Enter IP address of recipient for event messages.
Save configuration	
Read all Settings	Use the “Read” button to read all the EPA settings as AT commands. The settings can be copied from this window and saved or used in other programs.
Load configuration	

Table 2-2 Parameter list for Info page [...]

Designation	Description
Load Configuration	Load and execute configuration commands from a file. In combination with “Read all settings” the entire configuration can be restored.
Reload Settings	Read again all indications of the WBM fields from the EPA.
Write all	Transmit all the current settings to the EPA.
Reboot	Trigger reboot of EPA.
AT commands (only displayed in “Advanced View”)	
AT commands	
Send	Enter AT commands in the text box and transmit to EPA via “Send” button.
AT response	
(Text window)	Shows the AT commands and their responses.
Firmware update from TFTP	
Server IP Address	Enter IP address of the TFTP server that provides the firmware file.
File name	Enter name of the firmware file.
Update	Start firmware update. Ensure that TFTP transmission is not blocked by a firewall.

2.5 SSC script

Configuration via SSC script is the right option if a number of EPAs must be identically or similarly configured. A script can be executed on all current Windows PCs without any further installation. It allows for configurations that can be reproduced quickly and without errors.

SSC is based on the Windows Scripting Host (WSH) that has been an integral part of all current Windows versions since Windows 98.

For a detailed description containing examples, please refer to (SimpleScriptConfiguration _00.zip) at download.phoenixcontact.com.

2.6 Firmware update via Factory Manager

The firmware for the EPA module can be updated. The Factory Manager from Phoenix Contact can be used for this purpose.

The latest version can be downloaded at phoenixcontact.com.

- Start Factory Manager.

Add the FL BT EPA as a new device by right-clicking in the top window and selecting “Add device...” (“Gerät hinzufügen...”).

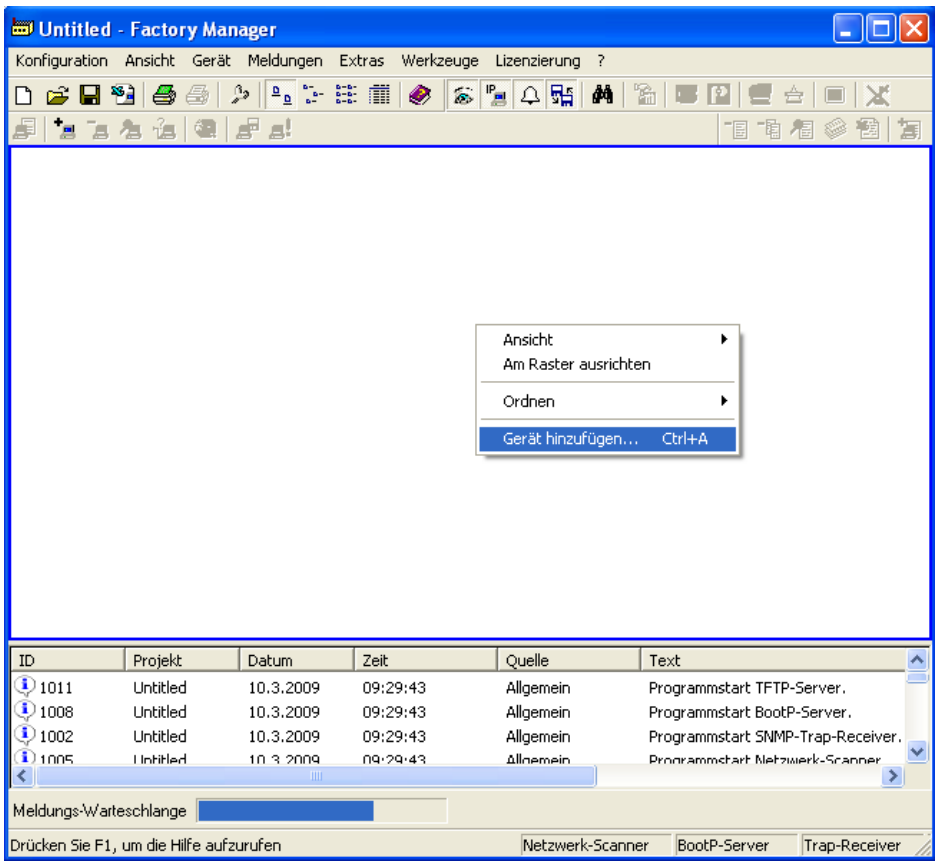


Figure 2-6 Adding the device in Factory Manager

In the window that appears, click on “BootP”.

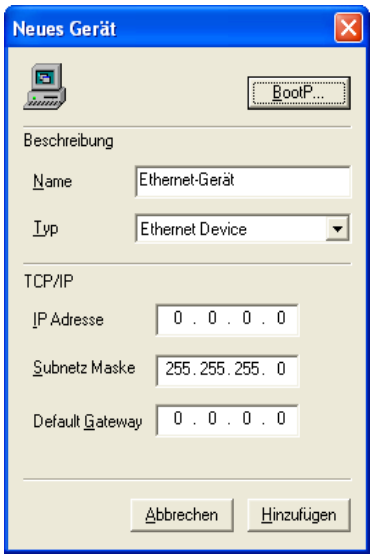


Figure 2-7 “New device” (“Neues Gerät”) dialog box in Factory Manager

In the “MAC address” field, enter the MAC address of the EPA module which can be found on the device label (MAC addr.: 00:12:f3:xx:xx:xx). Using the “Select” button, select the firmware file from the folder where you have previously saved the file. In the “TFTP server” field, enter your own IP address or select it with “Change”. Confirm the window with “OK”.

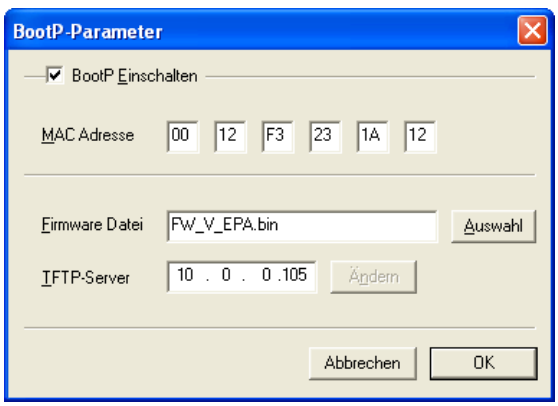


Figure 2-8 “BootP Parameters” (“Boot-Parameter”) dialog box in Factory Manager

In the “New Device” window, enter the IP address (default IP address 10.0.0.100) and the subnet mask (default 255.255.255.0) for the EPA module. Please note that the IP address of the PC and the EPA module must be in the same subnetwork.

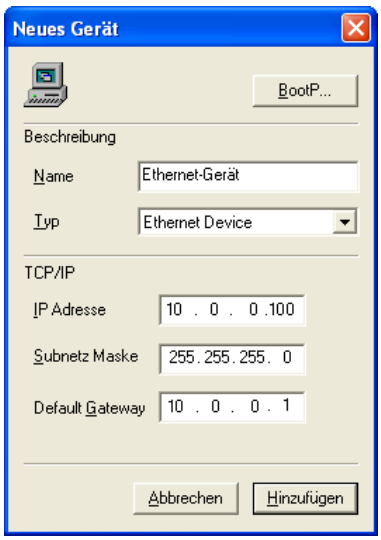


Figure 2-9 “New Device” (“Neues Gerät”) dialog box in Factory Manager

The newly created module now appears as a device in the main window of Factory Manager. Switch off the EPA module and then switch it on again with the MODE button pressed. The update should now be executed automatically on the EPA module. The progress is indicated in the bottom window of Factory Manager. Once the update is complete, the device can be started up with the new firmware in the usual way under the default IP address (10.0.0.100).

With the update installation, the EPA module loses all its current settings. The EPA module is now reset to the default settings.

3 Simple Network Management Protocol (SNMP)

3.1 General function

SNMP is a manufacturer-independent standard for Ethernet management. It defines commands for reading and writing information, and defines formats for error and status messages. SNMP is also a structured model that consists of agents, their relevant Management Information Base (MIB) and a manager. The manager is a software tool that is executed on a network management station. The agents are located inside switches, bus terminal modules, routers, and other devices that support SNMP. The task of the agents is to collect and provide data in the MIB. The manager regularly requests and displays this information. The devices can be configured by writing data from the manager to the MIB. In the event of an emergency, the agents can also send messages (traps) directly to the manager.

All configuration modifications, which are to take effect after a device restart, must be saved permanently.

SNMP interface

All managed Factoryline components have an SNMP agent. This device agent manages Management Information Base II (MIB 2) according to RFC1213 and private SNMP objects from the Phoenix Contact MIB (PXC-WLAN-MIB).
Network management stations, such as a PC with Factory Manager, can read and modify configuration and diagnostic data from network devices via the Simple Network Management Protocol. In addition, any SNMP tools or network management tools can be used to access Factoryline products via SNMP. To do this, the MIBs supported by the relevant device must be made available to the SNMP management tools.
On the one hand, these are globally valid MIBs, which are specified and described in RFCs (Request for Comments). This includes, for example, MIB2 according to RFC1213, which is supported by all SNMP-compatible network devices. On the other hand, manufacturers can specify their own SNMP objects, which are then assigned to a private manufacturer area in the large SNMP object tree. Manufacturers are then responsible for their own private (enterprise) areas, i.e., they must ensure that only one object is assigned to an object ID (object name and parameters) and can be published. If an object is no longer needed, it can be labeled as “expired”, but it cannot be reused with other parameters under any circumstances.
Phoenix Contact provides notification of ASN1 SNMP objects by publishing their descriptions on the Internet.
Reading SNMP objects is not password protected. However, a password is required for read access in SNMP, but this is set to “public”, which is usual for network devices, and cannot be modified. By default upon delivery, the password for write access is “private” and can be changed by the user.

For SNMP the password “public” is used for read-only access, the password “private” for read/write access.

Another benefit for the user is the option of sending traps using the Simple Network Management Protocol.

Management Information Base (MIB)

Database which contains all the data (objects and variables) required for network management.

Agent

An agent is a software tool, which collects data from the network device on which it is installed, and transmits this data on request. Agents reside in all managed network components and transmit the values of specific settings and parameters to the management station. On a request of a manager or on the occurrence of a specific event, the agent transmits the collected information to the management station.

Schematic view of SNMP management

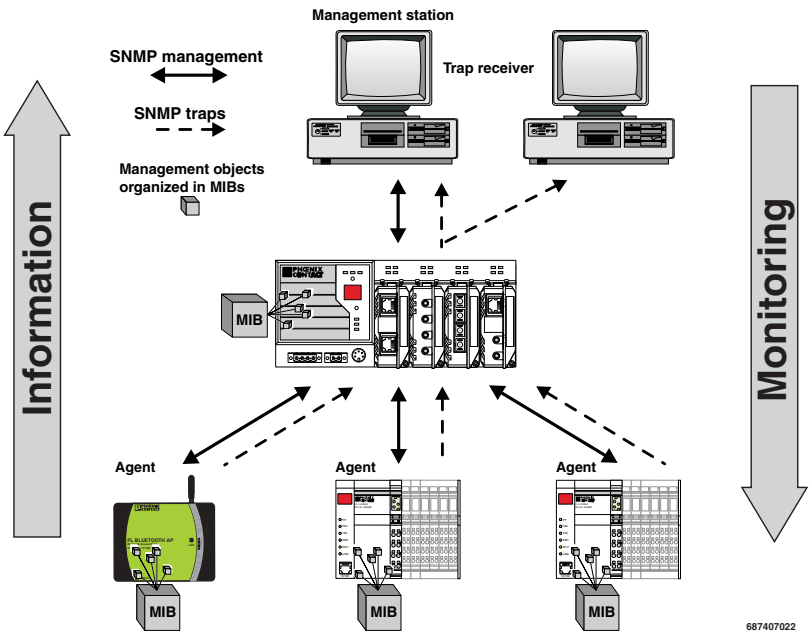


Figure 3-1 Schematic view of SNMP

3.2 Supported MIBs

The device supports MIB “RFC1213” and the “FL WLAN EPA”. The complete MIB files are available at phoenixcontact.com.

For SNMP the password “public” is used for read-only access, the password “private” for read/write access.

4 Additional information

4.1 Propagation of radio waves

4.1.1 Basics

Wireless technology is based on the propagation and receipt of electromagnetic waves. These waves are not subject to wear of any kind, but respond in very different ways in terms of propagation, dispersion, diffraction, and reflection depending on their frequency. The propagation of waves in an area is three-dimensional and occurs at different strengths.

Numerous factors affect this propagation, however none of these factors may affect the propagation to the extent that a signal is not safely detected at the recipient.

4.1.2 Propagation of radio waves outdoors (Fresnel zone)

Keep Fresnel zone free from any obstacles.

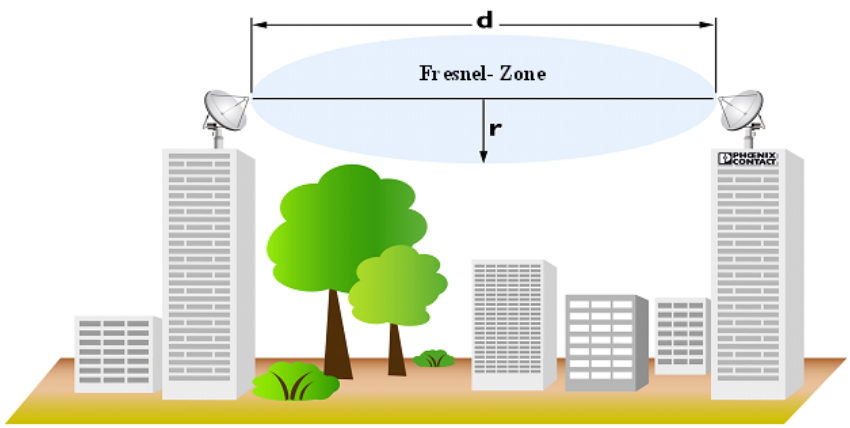


Figure 4-1 The Fresnel zone

4.1.2.1 Marginal conditions for planning a wireless path

There should be a line of sight, especially in the event of longer distances, between the antennas of the wireless devices. To keep the Fresnel zone free from any obstacles, it may be necessary to mount the antennas a few meters high. This area should also be free from any other obstacles.

Table 4-1 Fresnel zone - Mounting height for Bluetooth devices (antennas)

Wireless path distance (d)	Antenna height 2.4 GHz (r)
100 m	1.7 m
200 m	2.5 m
300 m	3.0 m
400 m	3.5 m

Note: The wireless path may also work if obstacles are within the Fresnel zone (house, tree, etc.). Usually, the decisive factor is the number of obstacles and the area they occupy in the Fresnel zone. However, there is no clear calculation basis for this. It is therefore recommended to perform test measurements.

Indoors: reflections (which do not occur outdoors in this way) usually dominate in the conventional automation environment and ensure a safe wireless connection even if the Fresnel zone is not free from obstacles.

4.1.3 Free space attenuation of the wireless signal/Fresnel zone

The following table lists the values for free space attenuation which experiences a wireless signal at different distances.

Keep the Fresnel zone free from any obstacles.

For Bluetooth the values apply for 2.4 GHz.

Table 4-2 Free space attenuation at 2.4 GHz

Distance in m	Attenuation at 2.4 GHz
5	54.0 dB
10	60.0 dB
20	66.0 dB
30	69.5 dB
50	74.0 dB
100	80.0 dB
110	80.8 dB
120	81.6 dB
150	83.5 dB
200	86.0 dB
250	88.0 dB
300	89.5 dB

Table 4-2 Free space attenuation at 2.4 GHz

Distance in m	Attenuation at 2.4 GHz
350	90.9 dB
400	92.0 dB
450	93.1 dB
500	94.0 dB
550	94.8 dB
600	95.6 dB
650	96.3 dB
700	96.9 dB
750	97.5 dB
800	98.1 dB
850	98.6 dB
900	99.1 dB
950	99.6 dB
1000	100.0 dB

Calculation for 2.4 GHz: free space attenuation [dB] = 100 + 20log distance [km]

4.1.4 Propagation of the radio wave indoors

4.1.4.1 In an industrial hall

If the wireless unit is installed in an industrial hall, the conditions listed above basically apply. The Fresnel zone will not be free there. However reflections on metal objects may promote the propagation of radio waves.

The range of the wireless modules depends on their mounting location and/or the position of their antennas.

In general the antenna should be free from other objects, so it can radiate well into the area. It should, for example, not be touched by cables or be surrounded by a metal control cabinet.

The reference value for the range within an industrial hall is up to 50 meters. The actual range may considerably exceed or fall below this value. This variation depends on the environment and the transmission power set. Large metal obstacles, such as walls or machines, may limit the range in that direction. This is particularly true if they are permanently located (static) between the wireless units.

The range can be limited by reducing the transmission power. Thus, only certain areas can be covered, if desired.

A more exact estimation of the range can also be achieved by prior simulation. The influence of the environment is then also taken into consideration. To do so, use the

FL Wireless Simulation Tool software (Order No. 2692254), which is available as an accessory.

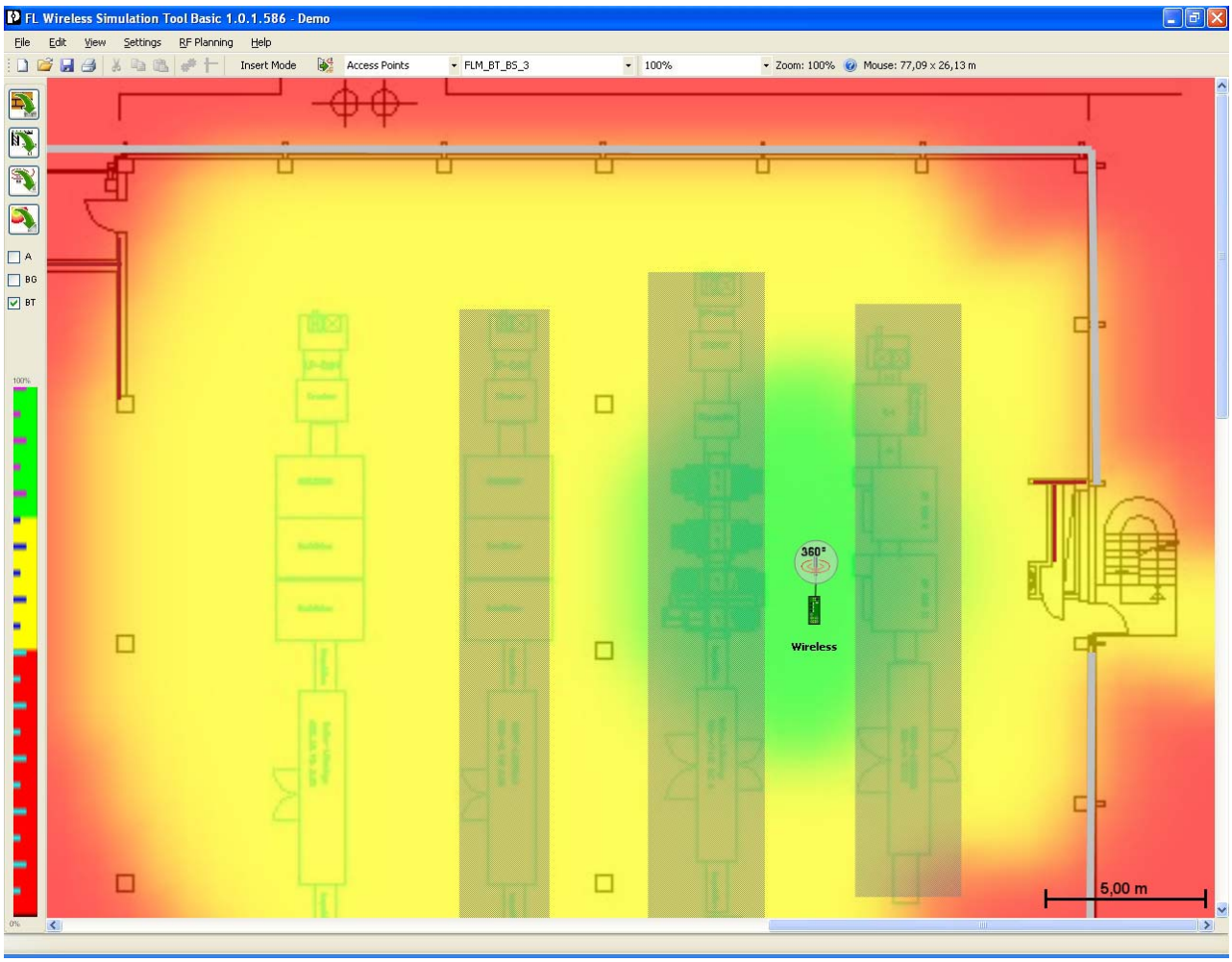


Figure 4-2 Representation of the radio propagation, taking into consideration the walls and machines in the simulation

4.2 PROFINET/PROFIsafe via Bluetooth

The PROFIBUS user organization has specified PROFIsafe for wireless transmission paths. Positive concept assessments have also been obtained from the BGIA (Professional Institute for Safety at Work) and TÜV (German Technical Inspectorate). The version of the PROFIsafe profile (version 2.4) describes the marginal conditions for the functionally safe transmission of data via WLAN and Bluetooth. In particular, security aspects for the configuration of wireless components and for safeguarding cyclic data exchange are specified. The FL BT EPA (MP) meets these requirements when it is operated in “4 / 6” or “8 / 9” oper-

ating mode. When configuring a PROFIsafe connection via Bluetooth, the additional latency of the wireless path must be taken into account. The PN update time should typically not fall below 32 ms. With several devices in a PAN, higher time values may be required.

To ensure a stable latency, the data load for a wireless path must never be higher than the transmission capacity of the wireless side. Problems rarely occur from the actual user data but sometimes from multicast or broadcast data. In time-critical applications we highly recommend to optimize data traffic using properly configured managed switches.

According to the PROFINET specification, FL BT EPA (MP)s react to PTCP packets by not transferring them. Operation with PN-IRT-capable devices is therefore possible without explicit PTCP filtering in front of the wireless path. We cannot guarantee proper functioning for PROFINET networks that do not comply with PROFINET specifications.

5 Technical data

General data	
Function	Bluetooth Ethernet adapter
Housing dimensions (width x height x depth) in mm	91 x 34 x 66
Permissible operating temperature	-40°C ... 65°C
Permissible storage temperature	-40°C ... 85°C
Degree of protection	IP65
Humidity	
Operation	5% ... 90%, non-condensing
Storage	5% ... 90%, non-condensing
Air pressure	
Operation	79.5 kPa ... 108 kPa, 2000 m above sea level
Storage	70 kPa ... 108 kPa, 3000 m above sea level
Mounting position	On a level mounting surface
Connection to protective earth ground	Not required
Weight	120 g, typical

Supply voltage	
Connection	Via M12
Nominal value	24 V DC (SELV)
Permissible voltage range	9 V DC ... 30 V DC
Typical current consumption at US at 24 V DC	46 mA
Power consumption, typical	1.2 W

Interfaces	
Number of Ethernet ports	1
Connection format	4-pos. M12 socket on the device (D-coded)
Connection medium	Twisted pair cable with a conductor cross section of 0.14 mm^2 ... 0.22 mm^2
Cable impedance	100 Ohm
Transmission speed	10/100 Mbps, auto negotiation
Maximum network segment length	100 m
Default IP address	10.0.0.100
Bluetooth interface	
Version	Bluetooth according to IEEE 802.15.1; 2.4 GHz to 1 Mbps
Transmission power	10 dBm, maximum - automatically controlled
Receiver sensitivity	-92 dBm
Wireless modules that can be connected	1 (standard), 7 (MP)
Supported profiles	PAN, PANU
FL BT EPA antenna	
Characteristics	Panel antenna (cannot be replaced), +5dBi
Connection	Internal
FL BT EPA MP antenna	External RSMA connection (female)

Interfaces [...]	
Operating mode	PANU, NAP
Configuration	Via web-based management, AT commands, script, MODE button
Security	128-bit data encryption, authentication, PIN, non-discoverable

Mechanical tests	
Shock test according to IEC 60068-2-27	Operation: 25g, 11 ms period, half-sine shock pulse Storage/transport: 50g, 11 ms period, half-sine shock pulse
Vibration resistance according to IEC 60068-2-6	Operation/storage/transport: 5g, 10 ... 150 Hz, Criterion 3
Free fall according to IEC 60068-2-32	1 m

Approvals

FCC/CFR 47 Part 15, ETS 300 328

Conformance With EMC Directives	
Noise emission according to EN 55022	Class B
Radio interference field strengths according to EN 55022	Class A
Electrostatic discharge (ESD) according to EN 61000-4-2	Contact discharge: ±4 kV Air discharge: ±8 kV
Electromagnetic fields according to IEC 61000-4-3	10 V/m; Criterion A
Conducted interference according to IEC 61000-4-6	10 V_{RMS}; Criterion A
Fast transients (burst) according to IEC 61000-4-4	Data lines: 1 kV; Criterion B Power supply lines: 0.5 kV; Criterion B
Surge voltages according to IEC 61000-4-5	Data lines: ±1 kV asymmetrical; Criterion B Power supply lines: ±0.5 kV symmetrical/asymmetrical; Criterion B

Differences between this version and previous versions

Rev. 00: First version

Rev. 01: Multiport devices integrated

5.1 Ordering data

5.1.1 Products

Description	Order designation	Order No.	Pcs. / Pkt.
Bluetooth Ethernet adapter	FL BT EPA	2692788	1
Set consisting of two modules and accessory cables	FL BT EPA AIRSET	2693091	1
Multiport Bluetooth Ethernet adapter	FL BT EPA MP	2701416	1

5.1.2 Accessories

Ethernet cables/description	Order designation	Order No.	Pcs. / Pkt.
Bus system cable, Ethernet, 4-pos., PUR, halogen-free, RAL 5021 (water blue), shielded, straight M12 plug (D-coded) to free cable end, cable length: 2 m	SAC-4P-M12MSD/ 2,0-931	1569391	1
Bus system cable, Ethernet, 4-pos., PUR, halogen-free, RAL 5021 (water blue), shielded, straight M12 plug (D-coded) to free cable end, cable length: 5 m	SAC-4P-M12MSD/ 5,0-931	1569401	1
Assembled Ethernet cable, CAT5e, shielded, 2-pair, 26 AWG stranded (7-wire), RAL 5021 (water blue), M12 plug to RJ45 plug/IP20, line, length: 1 m	VS-MSD-IP20-93E/1,0	1403498	1
Assembled Ethernet cable, CAT5e, shielded, 2-pair, 26 AWG stranded (7-wire), RAL 5021 (water blue), M12 plug to RJ45 plug/IP20, line, length: 2 m	VS-MSD-IP20-93E/2,0	1406056	1
Assembled Ethernet cable, CAT5e, shielded, 2-pair, 26 AWG stranded (7-wire), RAL 5021 (water blue), M12 plug to RJ45 plug/IP20, line, length: 5 m	VS-MSD-IP20-93E/5,0	1403500	1

Power supply cables/description	Order designation	Order No.	Pcs. / Pkt.
Sensor/actuator cable, 4-pos., PUR, halogen-free, RAL 7021 (black-gray), free cable end to straight M12 socket, A-coded, cable length: 1 m	SAC-4P- 1,0-PUR/M12FS	1400420	1
Sensor/actuator cable, 4-pos., PUR, halogen-free, RAL 7021 (black-gray), free cable end to straight M12 socket, A-coded, cable length: 2 m	SAC-4P- 2,0-PUR/M12FS	1533576	1
Sensor/actuator cable, 4-pos., PUR, halogen-free, RAL 7021 (black-gray), free cable end to straight M12 socket, A-coded, cable length: 3 m	SAC-4P- 3,0-PUR/M12FS	1668111	1
Sensor/actuator cable, 4-pos., PUR, halogen-free, RAL 7021 (black-gray), free cable end to straight M12 socket, A-coded, cable length: 5 m	SAC-4P- 5,0-PUR/M12FS	1668124	1

General accessories/description	Order designation	Order No.	Pcs. / Pkt.
Set for mounting devices with EPA design on a DIN rail	FL EPA RMS	2701133	1
Set for mounting devices with EPA design to wall or mast, including mast clips for a diameter of 25 - 85 mm, can be moved on two axes for optimum alignment, stainless steel	FL EPA WMS	2701134	1

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstr. 8
32825 Blomberg
Germany


+ 49 - (0) 52 35 - 3-00


+ 49 - (0) 52 35 - 3-4 12 00


phoenixcontact.com


Worldwide locations:
phoenixcontact.com/salesnetwork

HOTLINE:

If there are any problems that cannot be solved using this documentation, please call our hotline:


+ 49 - (0) 52 81 - 946 2888