

# ESCG

802.11 a/b/g

WLAN-Client Adaptor and Bridge

## Manual



**Content:**

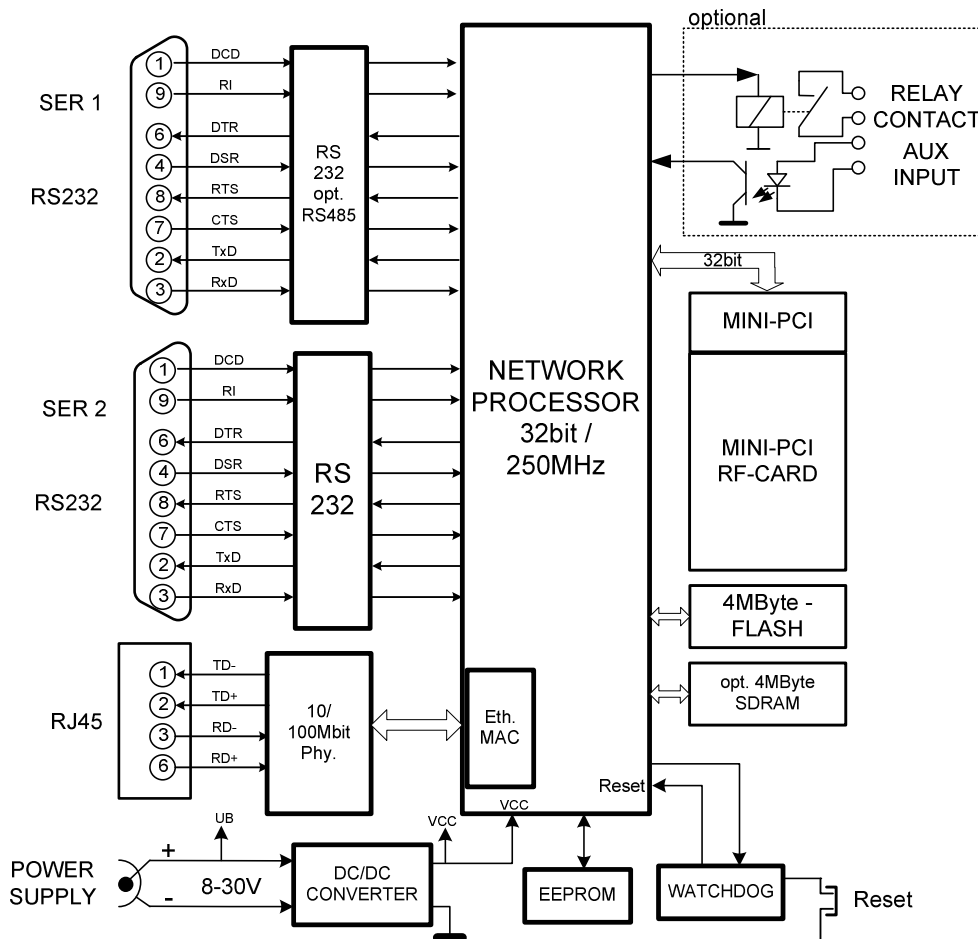
|   |    |
|---|----|
| <i>Overview</i> .....                                     | 3  |
| Technical features:.....                                  | 5  |
| WLAN - Interface:.....                                    | 5  |
| <i>First Time Setup</i> .....                             | 6  |
| The ESCG-Config Program .....                             | 6  |
| Reset to factory default .....                            | 7  |
| <i>Parameter setting via WEB interface</i> .....          | 7  |
| Information page .....                                    | 7  |
| Access Point page .....                                   | 9  |
| Security page .....                                       | 11 |
| Admin page .....  | 12 |
| Advanced page .....                                       | 13 |
| Cloning .....   | 13 |
| Advanced bridging.....                                    | 13 |
| Roaming .....   | 13 |
| Ethernet Port .....                                       | 13 |
| DHCP-Relay-Agent .....                                    | 13 |
| Serial interface setup .....                              | 15 |
| Comment to the multicast settings .....                   | 16 |
| Power supply connector.....                               | 19 |
| <br>Pictures:   |    |
| Illustration 1 Block schematic .....                      | 3  |
| Illustration 2 Connections and LEDs .....                 | 4  |
| Illustration 3 arrangement to configure the ESCG.....     | 6  |
| Illustration 4 screenshot of the ESCG-Config-Program..... | 6  |
| Illustration 5: Information page .....                    | 8  |
| Illustration 6: Access Point page .....                   | 9  |
| Illustration 7: Wireless page.....                        | 10 |
| Illustration 8: Security page .....                       | 11 |
| Illustration 9: Administration page .....                 | 12 |
| Illustration 10: Advanced page .....                      | 14 |
| Illustration 11: Windows TCP/IP port monitor.....         | 15 |
| Illustration 12: Multicast-mode.....                      | 16 |
| Illustration 13: Serial interface setup .....             | 18 |
| Illustration 14 Power supply connector.....               | 19 |

# Overview

The ESCG is intended to connect devices with ethernet or serial interfaces to a Wireless Local Area Network (WLAN) corresponding to the 802.11 a/b/g standard. The ESCG connects over the ethernet interface all devices in its LAN segment with a LAN that is accessible over WLAN.

The ESCG can receive and transmit data over its serial port which are exchanged over LAN or WLAN with other devices, i.e. another ESCG or a computer with a suitable software.

Functional blocks:



**Illustration 1 Block schematic**

The core of the ESCG is a 32bit network processor that controls all functions.

The interfaces:

- 1) Mini-PCI-Socket
- 2) Ethernet-Interface 10/100 MBit + auto MDI (auto crossover function)
- 3) 1 or 2 serial interfaces with 6 status lines each
- 4) optional: Relay contact and AUX input with optocouple

The ethernet port has a RJ45 input. Because of the auto MDI functionality the ESCG can be attached to a HUB or the LAN port of a computer with standard patch cables. The ESCG recognizes the cable polarity and automatically connects the right signal lines.

The serial port is a 9 pin female D-SUB connector. The pinout makes it possible to connect to a computer COM port with a 1 to 1 serial cable, the exact pinout is shown in Illustration 1 above.

The power supply should be 8 – 30VDC / 3W. At 12VDC the input current is 250mA.

Back and front view:

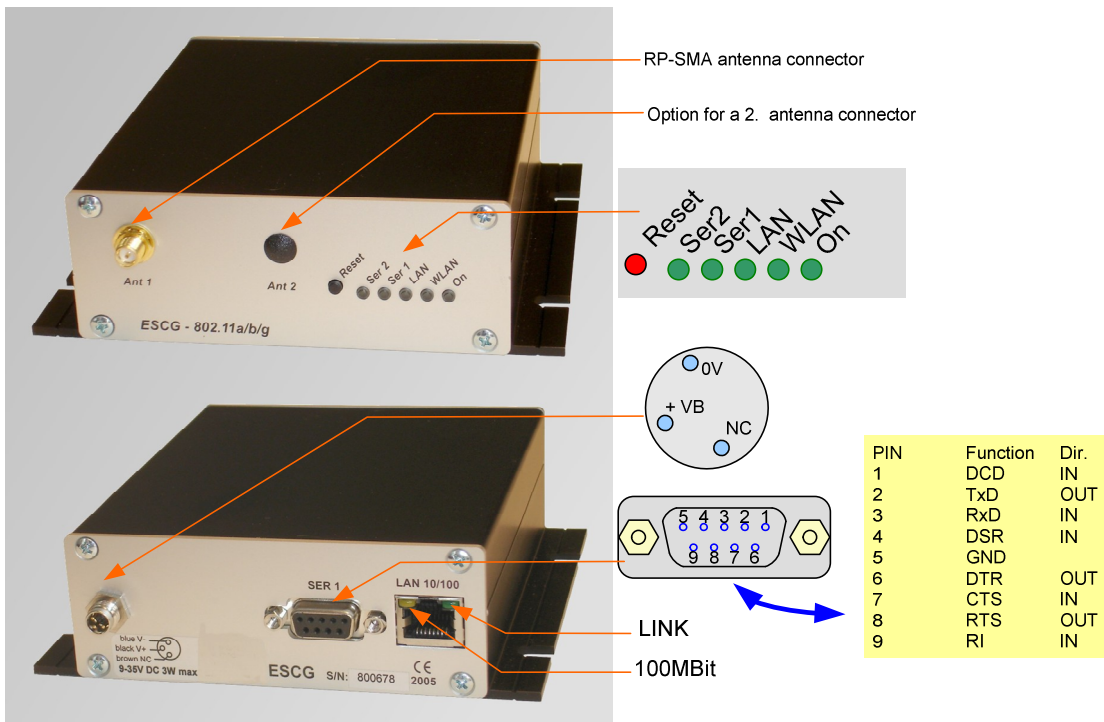


Illustration 2 Connections and LEDs

| LED      | Function                    |   |
|----------|-----------------------------|---|
| On       | <b>Green</b>                | always on when power is on  |
| WLAN     | <b>Red blinking</b>         | searching for RF-connection (scanning)  |
|          | <b>Steady green</b>         | found a suitable Access-Point and established a connection                    |
|          | <b>Green blinking</b>       | 802.1x Authentication is in process   |
|          | <b>Green + red blinking</b> | RF activity (receive or transmit)   |
| LAN      | <b>Off</b>                  | no link is recognized   |
|          | <b>Green</b>                | link is established with another LAN device.                                  |
|          | <b>Green + red blinking</b> | activity on the LAN interface   |
| Ser1 (2) | <b>Off</b>                  | interface is inactive or not connected to the other (W)LAN-communication side |
|          | <b>Green</b>                | connected to other serial device.   |
|          | <b>Green + red blinking</b> | activity on the serial interface (receive or transmit)                        |

## Technical features:

|                          |                      |  |
|--------------------------|----------------------|--|
| <b>Processor</b>         | Type                 | 32bit network processor 250MHz clock   |
|                          | Memory               | 256KByte program (internal)<br>64KByte data (internal)<br>4MByte flash (external)<br>4MByte SDRAM (external, optional) |
| <b>Interface</b>         | Ethernet             | 10/100 Mbps fast ethernet auto MDI/MDIX  |
|                          | Serial 1             | RS232 with control lines<br>RTS, CTS, DSR, DTR,DCD (input), RI (input)<br>(optional as RS485, RS422)                   |
|                          | Serial 2             | Same as serial 1 but only RS232  |
|                          | Mini-PCI             | Socket for RF cards with Atheros chipsets<br>(AR5112, AR5113)  |
|                          | Relay (optional)     | Relay contact<br>can be operated over LAN or WLAN<br>Connection with circular M8-4pin connector                        |
|                          | AUX input (optional) | Isolated input with optocouple   |
| <b>LEDs</b>              | LEDs                 | - Power (green)<br>- WLAN (green, red)<br>- LAN (green, red)<br>- SER1 (green, red)<br>- SER2 (green, red)             |
| <b>Power supply</b>      | Connector            | Standard: DC jack (2.1mm pin / 5.5mm hole)<br>optional: Circular M8-3pin connector with screw locking                  |
|                          | Power consumption    | < 2.5W (typ.) < 3W (max.)  |
|                          | Voltage range        | Standard: 8-30V non isolated<br>optional: 18-72V or 9-36V isolated   |
| <b>Temperature range</b> |                      | operating 0 - 70°C ( 32 - 158°F)<br>storage -20 - 80°C ( -4 - 176°F)   |
| <b>Dimensions</b>        | Board                | 120x100x20mm   |
|                          | Case                 | standard: 125x105x40mm   |
|                          | Weight               | approx. 500g   |

## WLAN - Interface:

|             |              |   |
|-------------|--------------|---|
| <b>WLAN</b> | Encryption   | 64, 128bit WEP, AES   |
|             | Security     | 802.11i WPA + WPA2 (Wifi Protected Access) (PSK/TKIP)<br>802.1x (EAP-TLS, EAP-PEAP), LEAP   |
|             | Data rates   | 802.11b 11, 5,5, 2 & 1 MBit/Sec.<br>802.11g 54, 48, 36, 24, 18, 12, 9, 6 MBit/Sec.<br>802.11a 54, 48, 36, 24, 18, 12, 9, 6 MBit/Sec.        |
|             | Frequencies  | ISM band: 2.400 MHz to 2.483 MHz<br>U-NII band: 5.150 MHz to 5.350 MHz (ETSI, RegTP indoor)<br>5.470 MHz to 5.725 MHz (ETSI, RegTP outdoor) |
|             | Channels     | 802.11b/g:<br>ETSI: 1-13, (3 non overlapping)<br>802.11a:<br>ETSI: 12 non overlapping (5.150-5.350 & 5.470-5.725 MHz)                       |
|             | Power output | 802.11b/g: 18dBm peak<br>802.11a: 18 or 17dBm   |

# First Time Setup

To set up the ESCG it has to be connected with a patchcable to the ethernet interface of a computer. Because of the auto MDI/MDIX capability, you can use a straight or crossover patchcable. After applying power, the green “Link LED” on the RJ45 connector shines when a link is detected. The yellow “100 MBit LED” indicates whether the connection is capable of 100 MBit. The “LAN” LED on the front panel shines green when a connection has been established over the ethernet. The “WLAN” LED on the front panel will be blinking red because usually no suitable WLAN is recognized.

## The ESCG-Config Program

To do the „first time setup“ the ESCG has to be connected via the LAN-Interface to the computer (PC) that runs the ESCG-Config-Program.

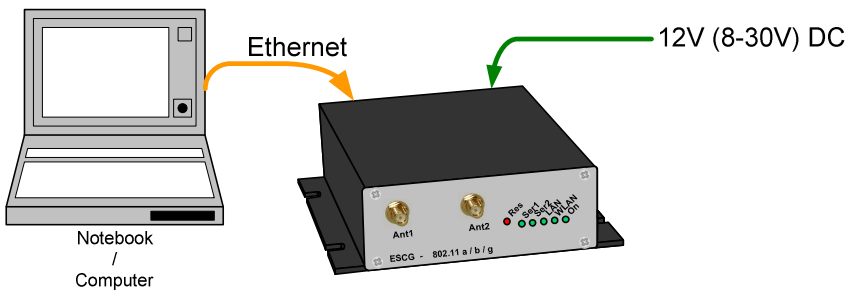


Illustration 3 arrangement to configure the ESCG

You have to observe:

- The connected PC should have an fixed IP address. (no DHCP)
- The LAN-Interface at the PC must be detected as connected. Check the parameter of the LAN-Interface with the „ipconfig“-command.
- If the LAN-Interface of the PC is correctly recognized then press the „refresh“-button of the ESCG-config-program.
- An active firewall could prevent the communication the ESCG.

After the start the ESCG-Config-Program ascertained all network interfaces that are active at the PC. After that the ESCG-Config-Program sends broadcast UDP requests to all these Interfaces. The registered answers of the ESCG devices are shown in a list.

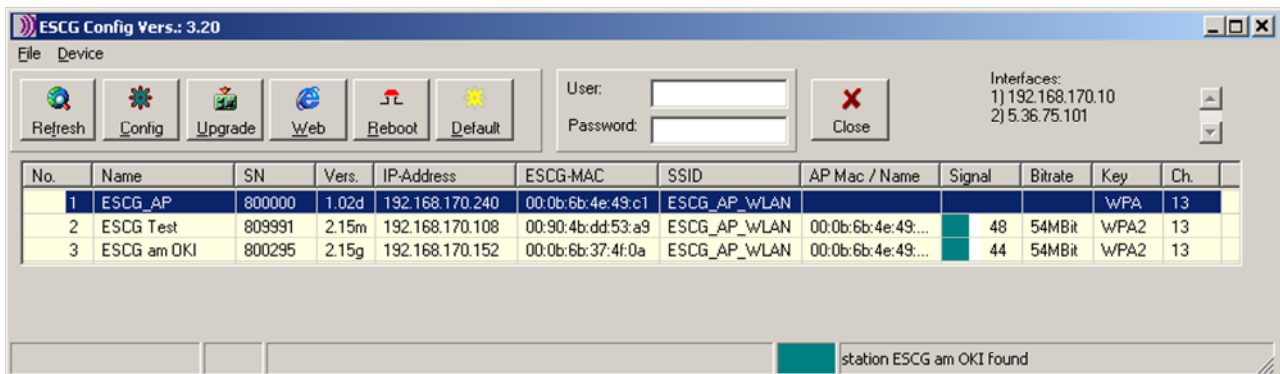


Illustration 4 screenshot of the ESCG-Config-Program

All located ESCG-Devices are shown in list with there station names, firmware versions and addresses. The WLAN connection is also shown with a signal quality value. The value can be interpreted as follows:

Signal  $\geq 40$  → connection very good

Signal  $\geq 30$  → connection good

Signal  $\geq 20$  → connection is ok, but the ESCG starts to search for better AP's.

Signal  $< 20$  → connection restricted, the bit rates will be lowered.

## ***Reset to factory default***

The factory default settings can be restored by pressing the reset button located on the front panel for a longer period. After about 5 seconds the LEDs "SER1" and "SER2" starts blinking red and green alternately. By keeping the button depressed the factory default values are restored. After finishing all LEDs except the "ON" LED are turned off. Now the reset button can be released.

main factory default values:

SSID = "ESCG\_WLAN"  
WEP = OFF  
WPA = OFF  
MODE= 802.11b/g

IP = 192.168.178.100  
Netmask = 255.255.255.0

SER1+2 : off  
802.1x user: „admin“  
802.1x password: „password“

## **Parameter setting via WEB interface**

### ***Information page***

General information regarding firmware versions and status reports

**ESCG**  
802.11 a/b/g  
WLAN Bridge

**funkwerk**  
enterprise communications

**Information**  
Information and Status  
NOTE: You may need to reload this page to see the current settings.

**Bridge Information**  
Serial Number: 802989  
Bridge Name: ESCG  
MAC Address: 000B6B4E49C1  
OS Software-Version: 6.3.5P (1019)  
Firmware-Version: ESCG 2.15m  
Device-Uptime: 0Days 00.00.23

**WLAN - Info**  
SSID: ESCG\_WLAN  
MAC-Addr. of AP: 0019A90ED1D0  
Current transmit rate: 54 Mbit/s  
Current channel: 1  
SNR: 30dB  
Security: None

**IP - Info**  
IP address: 192.168.170.107 (Static)

**Ethernet - Info**  
Link state: Up  
Link speed: 100 Mbit/s full duplex  
Connection type: straight through

**Serial Interfaces**  
Serial Port 1: COMSERVER Port: 8000  
Serial Port 2: not active

**Input / Output**  
Board-Relay: not active  
Input-Line: not active

**Callouts:**

- ESCG serial number
- Device name
- MAC address of internal RF card
- Firmware version
- Run time since switching on or last reset respectively.
- Network name (SSID)
- Used encryption: none, WEP, WPA
- Current ESCP IP address  
- static  
- DHCP = assigned by DHCP server
- Status LAN-Interface:  
Link state:  
„Up“ = connected  
„Down“ = no connection  
Link speed:  
- 100MBit full (half) duplex  
- 10MBit full (half) duplex  
Connection type:  
- straight through  
- crossed
- Setting and state of serial interfaces and AUX input / relay output if available.

**Illustration 5: Information page**

On the left hand side are links to different setup and info pages.

- Information the page above (Illustration 5)
- APs Shows a table with all access points currently seen by the ESCG (Illustration 6).
- Wireless WLAN interface setup (SSID, mode, frequencies etc.) (Illustration 7)
- Security Encryption setup (WPA, WEP) (Illustration 8)
- Admin
  - reboot ESCG
  - reset all parameters to default.
  - firmware updates
  - configure IP-address, subnet mask, gateway IP
  - configure setup options



- enter username and password  
(Illustration 9)

- serial Port 1 setup of serial port 1 (Illustration 13)
- serial Port 2 setup of serial port 2

## Access Point page

Information on all access points currently available to the ESCG.

The screenshot shows the ESCG web interface for the 'funktwerk' enterprise communications. The page title is 'Access Points' and it lists available access points. A table contains the following data:

| MAC address  | SSID              | Name         | Ch | Mode | RSSI | Time     | Last Seen |
|--------------|-------------------|--------------|----|------|------|----------|-----------|
| 0019A90ED1D0 | ESCG_WLAN         | CISCO_AP_250 | 1  | 11g  | 31dB | 1037 sec | 0 sec     |
| 020B6B33E78D | - Not available - | L-54A/G      | 3  | 11g  | 50dB | 0 sec    | 3 sec     |
| 060B6B33E78D | - Not available - | L-54A/G      | 3  | 11g  | 49dB | 0 sec    | 17 sec    |
| 0A0B6B33E78D | - Not available - | L-54A/G      | 3  | 11g  | 49dB | 0 sec    | 5 sec     |
| 000B6B33E78D | AP2000            | L-54A/G      | 3  | 11g  | 49dB | 0 sec    | 1 sec     |
| 0012BFACCAAF | WLAN-6A7C19       | - ????       | 1  | 11g  | 41dB | 0 sec    | 0 sec     |

Callouts from the image explain the following fields:

- SSID, Service Set Identifier:** This is the name of the access point and the connected open network. If the name is red, the ESCG is currently connected to it. Not available means the SSID is hidden (closed network).
- Access point name:** If not available: "???"
- Access points channel number:** (Points to the 'Ch' column)
- Access point mode:** 11b = 11MBit, 11g = 54MBit
- Connection time:** this shows how long the ESCG is or has been connected to that AP
- RSSI, Received Signal Strength Indication:** Indicates the signal strength for the reception from this access point. < 10 very poor, 10 - 20 poor, 20 - 40 good, >40 very good.
- Access point MAC address:** (Points to the 'MAC address' column)

Illustration 6: Access Point page

## Wireless page

Configuring the WLAN interface

The screenshot shows the 'Basic Wireless' configuration page for an ESCG device. The page title is 'funktwerk enterprise communications'. The main heading is 'Basic Wireless'. Below the heading, there is a note: 'On this page you can configure the basic 802.11a/g wireless settings. Any new settings will not take effect until the bridge is rebooted.' There are 'Save' and 'Cancel' buttons at the top right of the configuration area.

The configuration options are as follows:

- Wireless On/Off:** Radio buttons for ON (selected) and OFF.
- Wireless Mode:** Radio buttons for Infrastructure (selected) and Ad-hoc.
- Wireless Network Name (SSID):** Text input field containing 'ESCG\_WLAN'.
- Transmission rate (Mbits/s):** Dropdown menu set to 'Best (automatic)'.
- 802.11 Mode:** Dropdown menu set to 'Mixed 802.11g and 802.11b'.
- AP Density:** Dropdown menu set to 'low'.
- Super mode:** Dropdown menu set to 'Disabled'.
- Country:** Dropdown menu set to 'Germany'.
- Antenna Mode:** Radio buttons for Diversity (selected) and Single.
- 802.11a Frequency Bands:** Dropdown menu set to 'Band 1+2+3'.
- Channel:** Dropdown menu set to '2.412 GHz - CH 1'.

Callouts on the right side of the image explain the following settings:

- Switch the WLAN radio on or off:** Points to the 'Wireless On/Off' radio buttons.
- Wireless mode:** Infrastructure = Connect to AP; Ad hoc = peer to peer connection. Points to the 'Wireless Mode' radio buttons.
- SSID, Service Set Identifier:** Name of the WLAN network. This name must be the same as the access points SSID. Points to the 'Wireless Network Name (SSID)' field.
- Transmission rate:** Best = automatic depending on signal strength. If useful, you can select a fixed bitrate. Points to the 'Transmission rate (Mbits/s)' dropdown.
- 802.11 mode:** 802.11b = 2.4GHz 11MBit; 802.11g = 2.4GHz 54MBit; 802.11b/g = 2.4GHz 11 + 54MBit; 802.11a = 5GHz 54MBit. Points to the '802.11 Mode' dropdown.
- AP Density:** influences the roaming behaviour. Points to the 'AP Density' dropdown.
- Super mode:** is not supported. Points to the 'Super mode' dropdown.
- Country:** Select the country in which the ESCG is used. This determines the number of available channels. Points to the 'Country' dropdown.
- Antenna mode:** single = when one antenna is used; diversity = when two antennas are used. With two antennas the radio can select the antenna that delivers the best signal. Points to the 'Antenna Mode' radio buttons.
- 802.11a Frequency Bands:** possible channel restriction for the 5GHz (802.11a) operation. Points to the '802.11a Frequency Bands' dropdown.
- Channel:** This channel has to be selected in ad hoc mode only. Points to the 'Channel' dropdown.

### Illustration 7: Wireless page


By clicking the "Save" button all changes on this page are stored. Use "Cancel" to undo any changes. After clicking "Save" the program prompts the user to make a reboot. This should be done after all necessary changes on all pages have been made.

## Security page

Setting up the security options

If the user selects the 802.1x authentication the PSK or the WEP-Keys don't have to be defined because the ESCG and the Radius-Server will determine these parameters automatically.

**ESCG**  
802.11 a/b/g  
WLAN Bridge



**funkwerk**  
enterprise communications

**Information APs**

**Wireless Security Admin Advanced**

**Serial Port 1 Serial Port 2**

### Security and Encryption Settings

On this page you can set the 802.11a/g security and encryption options. Any new settings will not take effect until the bridge is rebooted.

**802.1x configuration**  
Enable 802.1x to require stations to use Authentication over EAP.

802.1x Authentifikation

EAP Mode EAP-PEAP  
Select the 802.1x Method.

802.1x user admin

802.1x password XXXXXXXXXX

**WPA configuration**  
Enable WPA Authenticator to require stations to use high grade encryption and authentication.

WPA Enable

WPA Mode WPA  
Select the WPA Mode.

Cipher Type TKIP  
Select the cipher type.

PSK XXXXXXXXXX  
Enter a text pass phrase between 8 and 63 characters.

**WEP configuration**  
WEP is the wireless encryption standard. To use it you must enter the same key(s) into the bridge and the access point. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. If you leave a key box blank then this means a key of all zeros.

Enable WEP

Check this box to enable WEP. For the most secure use of WEP, also set authentication type to "Shared Key" when WEP is enabled

Default WEP key to use WEP Key 1  
Select the key to be used as the default key. Data transmissions are always encrypted using the default key. The other keys can only be used to decrypt received data.

Authentication Open  
Select the type of authentication used when connecting to an access point. 'Open' is used if anyone can connect to the AP. 'Shared key' is used if both devices must know the encryption key. 'Network EAP' is only used in combination with 'EAP-LEAP'

WEP key lengths 64 bit (10 hex digits)  
Select the WEP key size. This length applies to all keys.

WEP key 1 XXXXXXXXXX

WEP key 2 XXXXXXXXXX

WEP key 3 XXXXXXXXXX

WEP key 4 XXXXXXXXXX

Enable authentication with radius server

Select authentication method 1  
EAP-PEAP  
EAP-TLS  
EAP-TTLS  
LEAP (CISCO spec.)

Username and Password

Enable WPA and select WPA mode  
WPA = encryption with RC4  
WPA2 = encryption conforming to AES

Select cipher type

PSK = Pre Shared Key for authentication with access point

Default WEP key for data transmission

Authentication type for registration with an access point

WEP key length  
64 bit or 128 bit

Enter keys as hex digits  
10 digits for 64 bit WEP  
26 digits for 128 bit WEP

There must be at least the one key that is defined as default WEP key

Illustration 8: Security page

# Admin page

Setting up administration rights and configure basic features, update firmware

**ESCG**  
802.11 a/b/g  
WLAN Bridge

**funkwerk**  
enterprise communications

**Administration**

On this page you can configure the IP address used by the Web server running on this bridge. For "static" mode, the IP address settings are given here. For "DHCP" mode, these settings are supplied by a DHCP server on your network. You can also change the password, reboot the bridge, or reset all settings to their factory defaults. If you have changed any settings it is necessary to reboot the bridge for the new settings to take effect.

**Device Control**

Clicking the button below will immediately reboot the device. A reboot is necessary in order to change most configuration options.

**Reboot**

Clicking the button below will reset all configuration options to their factory default values and the device will reboot. Note that the IP address of the device will also be reset and it may be necessary to change the address in your browser to access this website again.

**Reset Configuration**

**Firmware Upgrade**

To upgrade the firmware, enter the name of the firmware upgrade file, and click on the upgrade button below.

File to upload:  **Durchsuchen...**

**Upload**

The upload may take up to 60 seconds.

**Save** **Cancel**

**Device name**

Device name:

This is the name that the bridge will use to identify itself to external configuration and IP-address-finding programs. This is not the same as the SSID. It is okay to leave this blank if you are not using these programs.

**IP settings**

IP Address Mode:  Static  DHCP

Select 'DHCP' to get the IP settings from a DHCP server on your network. Select 'Static' to use the IP settings specified on this page.

Default IP address:

Type the IP address of your bridge

Default subnet mask:

The subnet mask specifies the network number portion of an IP address. The factory default is 255.255.255.0.

Default gateway:

This is the IP address of the gateway that connects you to the internet.

**Config options**

IP Config over UDP 41233:  Check this box to enable AutoIpConfig.

Telnet-Config:  Check this box to enable Telnet-Config.

UDP 9094 Config:  Check this box to enable Config over UDP-Port 9094.

disable wireless config:  Check this box to disable config over WLAN.

**Bridging options**

disable Bridge:  Check this box to disable the connection of the LAN Connector to the WLAN System.

**Security**

User name:

This is the user name that you must type when logging in to these web pages.

Administrator password:

This is the password that you must type when logging in to these web pages. You must enter the same password into both boxes, for confirmation.

**Callouts:**

- ESCG neu starten
- Restore ESCG configuration to default values
- Select firmware file
- Upload firmware to ESCG
- Device name: This is a name to identify the ESCG by external configuration and IP address lookup programs, i.e. the locator program. This is not the SSID
- IP address: By selecting "DHCP" the ESCG is assigned the IP address from a DHCP server on the network. By selecting "Static" the IP address is fixed. In this case the network mask has to be defined and possibly the default gateway.
- Enable more configuration options:
  - IP Config over UDP 41233:** assignment of an IP-Address over the LAN-Interface (special function).
  - Telnet-Config:** Configuration option via an telnet server socket (TCP-Port 23). Is Interface is compatible to the ESC-Config-Programm of the older 11MBit-ESG device
  - UDP 9094 Config:** Konfigurations-Option via UDP-Port 9094
  - disable wireless config:** for security reasons it is possible to prevent the configuration via WLAN.
- Option to block the bridging funktion of the ESCG. This could be useful when the ESCG only works as a serial client adapter. The configuration via LAN-Interface is not blocked with this option.
- Enter user name and password to protect the ESCG from unauthorized access

Illustration 9: Administration page

## ***Advanced page***

The advanced page offers more detailed options to define the behaviour of the ESCG in the WLAN environment.

### **Cloning**

The cloning parameter defines the MAC address of the ESCG's radio. Usually the ESCG leaves the MAC address at the manufacturers value. All devices connected to the WLAN over the ESCG's ethernet port use this MAC address for communication.

The ESCG keeps a table where the original MAC address of the connected device is linked to its IP address. If a data package arrives at the ESCG on the ethernet port, the ESCG first checks if there is an entry in its table with the source MAC address of this device. If the answer is no, this MAC address is added to the table.

Next it checks if there is an entry for the target MAC address.

If the answer is yes it means that the receiver of this data packet is located on the wired side of the ESCG and therefore there is no need to send it over the wireless radio.

If the answer is no, the source MAC address is replaced by the radio's MAC address and the data package is sent over the radio to the WLAN

If the ESCG receives a data package from the WLAN, it first extracts the target IP address. Next it looks up the corresponding MAC address in its table. This MAC address is placed in the data package which is then sent over the ethernet port to the connected devices.

With this method several devices can be connected to the ESCG.

This procedure only works in LAN's / WLAN's that use the IP protocol. If other protocols are used, the ESCG can be forced to transfer the MAC address of the first data packet that arrives on the ethernet port to the radio. This method is called cloning. It ensures that all data packages intended for the connected device are received by the ESCG. The ESCG can forward the data to the ethernet port without any further processing.

This method allows only one device to be connected to the ESCG ethernet port. This strategy is activated by selection the option "Eth. Client (var)".

With the option "Eth. Client (fixed)" the user can defined a MAC address that the ESCG will use for the WLAN Connection.

### **Advanced bridging**

Check this box to disable the data exchange between ESCG and WLAN. Some WLAN-Systems don't accept that 2 different IP addresses are working with the same MAC-Address. If you check this box, only the IP-Address of the Client that is connected to the LAN-Port will appear on the WLAN side. The configuration of the ESCG over WLAN is not possible with this setting.

### **Roaming**

Roaming is the term for automatically changing to another access point when the ESCG recognizes a decreasing RF signal level when leaving the covered area of the current access point and a better level with another AP available.

For this purpose the ESCG keeps a table with a list of access points from which it is receiving signals (beacons).

To receive these beacons the ESCG has to tune to the different channels and listen for incoming signals for a certain amount of time. This hampers the regular data traffic which the ESCG has to process. Therefore this procedure is handled in different ways depending on the current signal level.

To make this procedure even more effective, the user can restrict the channels where the ESCG is allowed to look for beacons of other access points

### **Ethernet Port**

Check this option to enable manual settings for the ethernet port.

### **DHCP-Relay-Agent**

Check this option to enable the DHCP-Relay-Agent of the ESCG. This is useful if the connected clients at the ethernet port of the ESCG are using DHCP.

Advanced

On this page you can configure the advanced 802.11a/g wireless settings. Any new settings will not take effect until the bridge is rebooted.

Save Cancel

Cloning

Cloning mode  WLAN Card  Eth. Client (var.)  Eth. Client (fixed)  
 This feature controls the MAC Address of the Bridge as seen by other devices (wired or wireless).  
 If set to "Ethernet Client (var)", the MAC address from the first Ethernet client that transmits data through the Bridge will be used. This setting is useful if there is only one Ethernet device connected to the Bridge.  
 If set to "Ethernet Client (fixed)", the MAC Address that is given in the Parameter "Fixed Client MAC" will be used.  
 If set to "WLAN Card", the MAC Address of the WLAN Card will be used (default).

Fixed Client MAC

Advanced bridging

detach ESCG IP from WLAN   
 Check this box to disable the data exchange between ESCG and WLAN. Some WLAN-Systems don't accept that 2 different IP addresses are working with the same MAC-Addr. If you check this box, only the IP-Address of the Client that is connected to the LAN-Port will appear on the WLAN side. The configuration of the ESCG over WLAN with "ESCG-Config" or WEB is still possible when you define the Ethernet-Client-IP.

Ethernet Client IP   
 IP Address of the Client connected to the LAN-Port. Set to "0.0.0.0" if unknown or variable

Alternative webservers port   
 Alternative webservers port for the web interface via WLAN <http://ClientIP.AlternativePort>

Advanced wireless

Scan dwell   
 This is the time in milliseconds that the device is waiting for answers after the sending of requests to accesspoints. The longer this time the longer a complete scan of all channels takes. The valid range is 10..200. Default is 20ms

Fragmentation threshold   
 Transmitted wireless packets larger than this size will be fragmented to maintain performance in noisy wireless networks. The valid range is 256..65535. Values larger than about 1560 will prevent fragmentation from taking place.

RTS threshold   
 Transmitted wireless packets larger than this size will use the RTS/CTS protocol to (a) maintain performance in noisy wireless networks and (b) prevent hidden nodes from degrading performance. The valid range is 1..65535. Values larger than about 1560 will prevent RTS/CTS from taking place.

Burst time   
 Set the time duration here for transmission burst mode, in microseconds. The valid range is 0..65535 with 0 to disable bursting. Burst mode can increase data throughput by occupying the channel for an extended duration. Typical values are in the range of several milli-seconds (ie. 3000).

Beacon period   
 In adhoc mode beacons are sent out periodically. This is the number of milliseconds between each beacon. The valid range is 1..65535.

802.11d   
 Check this box to enable support for receiving regional information from the access point.

Roaming

Channels for Roaming   
 Set the channels which the infrastructure system (AP's) use. So the ESCG can optimize the roaming. Input the channel numbers separated with ','

Ethernet Port

Manual Config   
 Check this box to enable manual settings for the ethernet port.

Bitrate  10 Mbit/s  100 Mbit/s  
 Duplex: Selection  half duplex  full duplex  
 LAN Cable Type  straight through  crossed

DHCP Relay Agent

DHCP Relay Agent   
 Enable DHCP Relay Agent for the devices connected to the LAN Port.

Illustration 10: Advanced page

## Serial interface setup

The ESCG can have one or two serial interfaces, depending on the options. Each interface is configured on its own WEB page.

### Network configuration

There are different modes available for the use of the serial interfaces:

1) **TCP/IP server mode:**

In this mode the ESCG opens a socket in a “listen mode”, which means that it is waiting on a certain port (local port) for a connection. The ESCG only holds one connection at a time. In this mode only the port number has to be specified.

2) **TCP/IP client mode:**

In this mode the ESCG actively opens a TCP connection on the specified port of another network node. This node can be another ESCG or a computer which is waiting for a connection on the specified port. In this mode the port number and the IP address of the connected device have to be specified.

3) **UDP/IP mode:**

In this mode the ESCG is waiting for data on the “local port“ which are sent with UDP/IP. The received data are then sent to the “remote port” of the remote IP address. The UDP should be used in circumstances where the communication between the devices is frequently interrupted. It should be considered though that the UDP protocol does not guarantee the correct transfer of data.

4) **Printerserver mode:**

In this mode the ESCG starts a TCP/IP socket in server mode which is waiting for a connection on port 515. The ESCG is then able to execute print jobs corresponding to RFC1179. If you want to enable a printer with this method under Windows, it has to be set up like the following example:

Example:

Windows setup for a printer connected over LPR

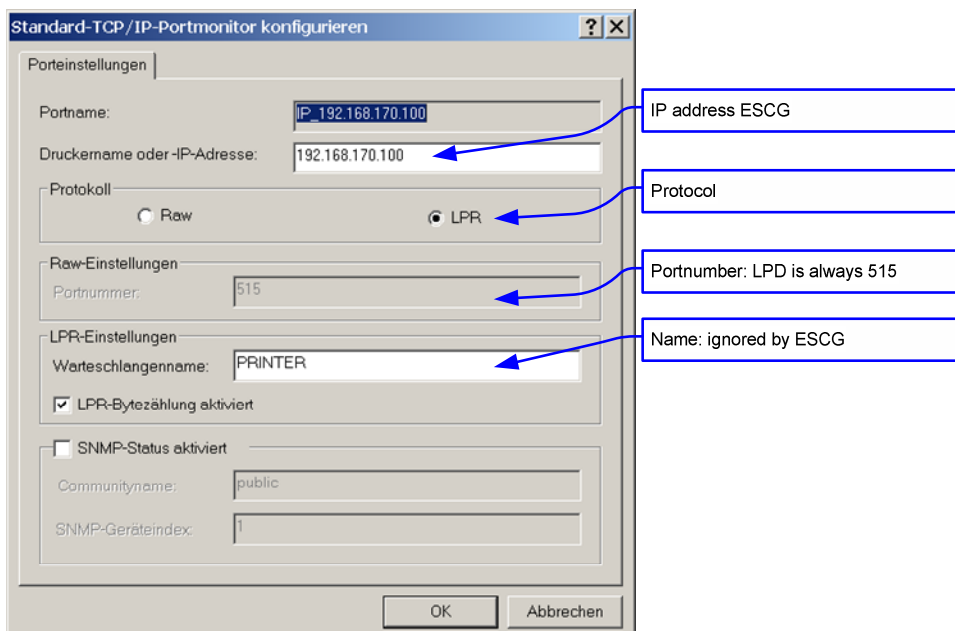


Illustration 11: Windows TCP/IP port monitor

5) **COM server mode:**

In this mode the ESCG provides virtual COM ports under Windows. For this purpose a software tool from the company Wiesemann & Theis ([www.wut.de](http://www.wut.de)) has to be installed. The tool is named “COM Umlenkung. This tool enables the ESCG to connect to serial devices over LAN/WLAN. After installation of the software enter the ESCG IP address and port number.

## Comment to the multicast settings

In the Multicast-Mode serial busmembers who are communicating with RS485 interfaces can be connected via the (W)LAN. Depending which task the serial device takes it is possible to configure different modes:

1. Slave
2. Master
3. Multimaster

As a slave the ESCG receives data on the configured multicast address and sends this data to the serial interface. Data that is received from the serial line is sent to the given unicast IP address.

As a master the ESCG receives data from the unicast IP address and transmits data to the multicast IP address.

In multimaster mode all transfers are done via the multicast IP address.

sample application:

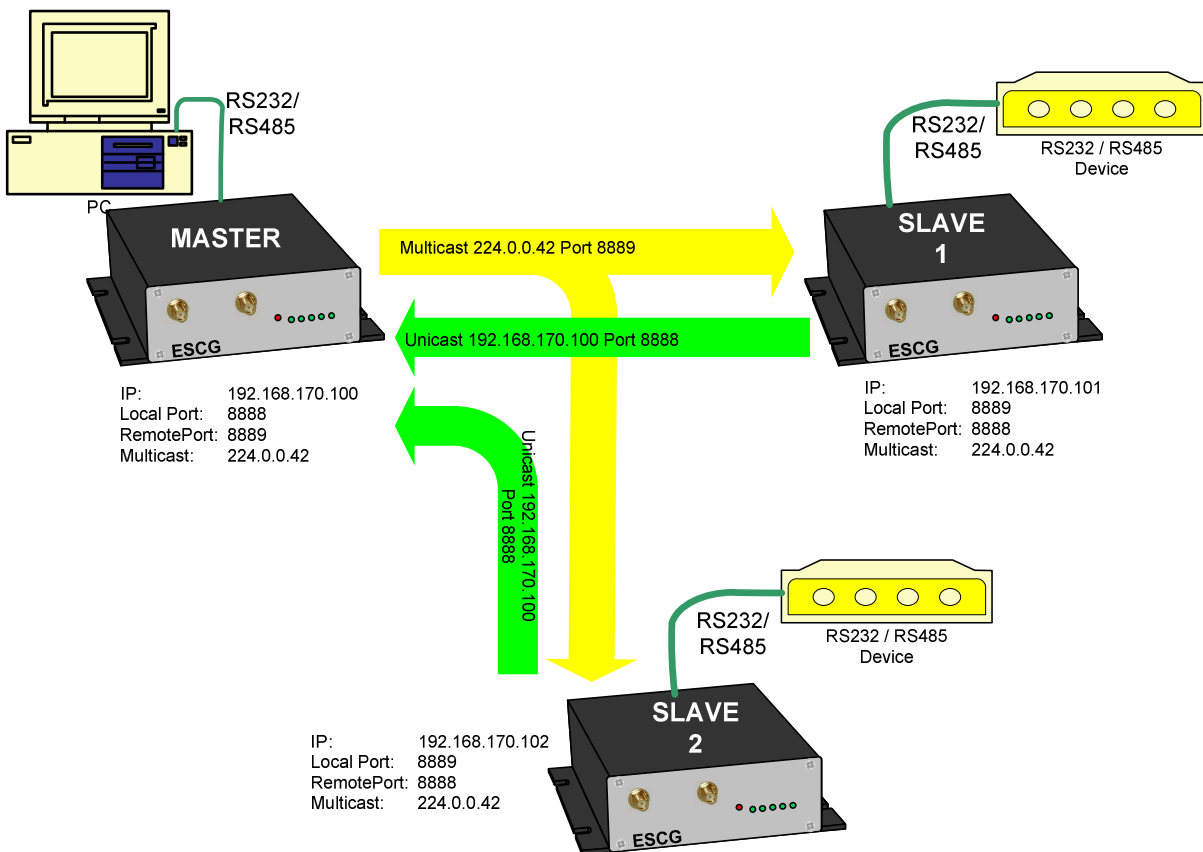


Illustration 12: Multicast-mode

## “Keep alive“ settings

A TCP/IP connection remains open after being established until one of the communicating devices closes the connection. If the physical connection between the ESCG and the other device is interrupted without closing the TCP/IP connection, there is a possibility that the ESCG is not able to reconnect. The TCP/IP socket can be programmed to send an empty data package to the communication partner in regular intervals (keep alive period). If the communication partner supports this mode, it sends a corresponding answer. This answer is proof that the connection is still intact. If there is no answer for a number of times (keep alive probes), the TCP/IP connection is closed and the ESCG starts the TCP/IP socket again.

## “Send trigger“ configuration



The data received by the ESCG are first temporarily stored. There are different criteria when the stored data will be sent over the LAN/WLAN.

- 1) **Byte trigger:** The user defines a number of Bytes. After reaching that number, the stored data are sent.
- 2) **Timeout:** After receiving a character a timer with the programmed value is started. Each received character restarts the timer. Once the timer has elapsed the stored data are sent.
- 3) **Delimiter:** The user defines a certain character. When this character is received, the stored data are sent.

The parameter “**receive fifo size**” defines the quantity of bytes that can be stored in a ringbuffer before the data is sent to the (W)LAN interface. If you use the ESCG in an application that receives permanently data via the serial interface the “receive fifo size” has to be set to a value between 1024 and 2048 bytes. Because the ESCG needs all the available RAM memory in a situation of authentication with 802.1x (PEAP, TLS) this value is set to a value of 256Bytes by default to save memory space.

### Handshake mode

This defines how the communication partners are signalling their ability to send and receive data. With the status lines RTS and DTR the ESCG reports that it is ready to receive. The status lines CTS and DSR are inputs where the communication partner reports its readiness to receive. The signals DCD and RI can be forwarded to the ESCGs LAN/WLAN communication partner.

The ESCG be controlled remote or local to handle the data flow.

The following modes are available to the user:

- 1) **no handshake:** The CTS/DSR signals are not utilized. CTS/RTS are set to active when the serial interface is connected over the LAN/WLAN.
- 2) **XON / XOFF :** The ESCG sends and receives the control characters XON = 0x11 and XOFF = 0x13. The ESCG sends a XOFF to his serial communication partner when the memory buffer is almost full and a XON when it is almost empty.
- 3) **RTS/CTS:** The ESCG signals that it is ready to receive over the RTS line and recognizes the CTS signal to determine if its serial partner is ready to receive.
- 4) **DTR/DSR:** The ESCG signals that it is ready to receive over the DTR line and recognizes the DSR signal to determine if its serial partner is ready to receive.
- 5) **Remote:** In this mode the ESCG transmits the state of the status lines CTS, DSR, RI and DCD to its LAN/WLAN communication partner. This happens over a different socket (port). This makes it necessary for the user to enter more specifications.

The state of the status lines are described by strings of letters.

A capital letter means the signal is active, a small letter means inactive.

|                  |                    |
|------------------|--------------------|
| 'D' = DSR active | 'd' = DSR inactive |
| 'R' = CTS active | 'r' = CTS inactive |
| 'C' = DCD active | 'c' = DCD inactive |
| 'I' = DSR active | 'i' = DSR inactive |

The ESCG interprets the received data as follows:

'D' -> set DTR to active            'd' = set DTR to inactive

'R' -> set RTS to active            'r' = set RTS to inactive

'C' or 'c' and 'I' or 'i' are ignored.

- 6) **3964R:** This is a special protocol which is commonly used for communication with SPS (programmable control systems). This protocol uses special characters and events to signal when it is ready to transmit and receive. Descriptions of this protocol are available in literature.

**ESCG**  
802.11 a/b/g  
WLAN Bridge

**funkwerk**  
enterprise communications

**Serial Client on Port 1**  
On this page you can configure the serial client on port 1. Any new settings will not take effect until the bridge is rebooted.

Information  
APs  
Wireless  
Security  
Admin  
Advanced

Serial Port 1  
Serial Port 2

Save Cancel

Port active  Check this box to enable this serial port.

**Port 1 baudrate and format**

Baudrate: 19200 Baudrate for this serial Port

Paritybit: none Select the parity bit.

Databits: 7 Select the number of databits

Stopbits: 2 Select the number of stopbits.

**Port 1 network configuration**

Port mode: TCP/IP server Select the port mode.

Server IP: 192.168.170.242 Server IP in client mode

Local port: 8888 Local port number

Remote port: 8888 Remote port number

**Port 1 multicast configuration**

Multicast mode: no multicast no multicast = send + receive unicast  
Slave = receive multicast, send unicast  
Master = receive unicast, send multicast  
Multimaster = receive multicast, send multicast

Multicast IP address: 224.0.1.42

**Port 1 keep alive parameter**

keep alive period: 0 Time between two "TCP keep alives" in seconds.

keep alive probes: 0 Amount of "keep alive probes" - failure till the TCP connection is closed.

**Port 1 send trigger configuration**

Byte trigger: 128 Number of bytes in the receive buffer to trigger the network sendroutine.

Character timeout: 10 Timeout in milliseconds between 2 characters to trigger the sendroutine.

Frame end delimiter:  This is a single HEX value. When the delimiter byte is received the receivebuffer will be send.

Receive FIFO size: 256 Receive FIFO size in bytes. The receive FIFO stores the bytes before they are send to the network (WLAN or LAN) interface. because of the limited memory space of this device you should take the lowest possible value.

**Port 1 handshake mode**  
XON/XOFF, RTS/CTS or DTR/DSR are local handshake modes. In "transparent mode" the status of the handshake input signals (DSR+CTS) will be send to the remote side via an extra port. 3964R means that the serial port handles this protocol for sending and receiving data

Handshake protocol: no Handshake Select the method of doing the handshake.

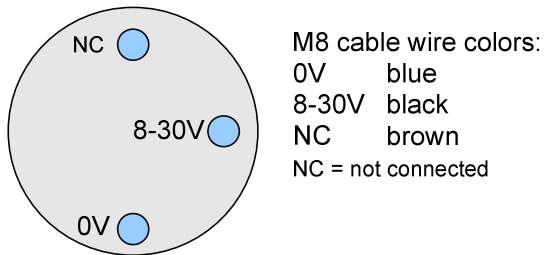
Local port: 8880 Local port number for handshake.

Remote port: 8880 Remote port number for handshake.

**Illustration 13: Serial interface setup**

## ***Power supply connector***

Optional the ESCG can be equipped with a circular M8- 3pin connector. The connection is as follows:



**Illustration 14 Power supply connector**

# Wireless LAN and your health

The Funkwerk Enterprise Communications Wireless LAN products, like other radio devices, emit radio frequency electromagnetic energy. The level of energy emitted by Wireless LAN devices however is far much less than the electromagnetic energy emitted by wireless devices like for example mobile phones. Because Wireless LAN products operate within the guidelines found in radio frequency safety standards and recommendations, Funkwerk Enterprise Communications believes Wireless LAN is safe for use by consumers. These standards and recommendations reflect the consensus of the scientific community and result from deliberations of panels and committees of scientists who continually review and interpret the extensive research literature.

## Federal Communication Commission Interference Statement

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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.

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.

The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

This device supports FCC Part 15, subpart E dynamic frequency selection (DFS client without radar detection). For the band 5150–5250 MHz this equipment must be used indoors only to reduce potential for harmful interference to co-channel mobile satellite systems.