Installation and Operating Manual

(Translation of the original installation and operating manual)

OnSens.SmarTemp
Self-Contained Non-Contacting Thermal Measuring Device

Version 1, 2026-05-05
3201-014141 en, Protection Class 0: public

Contact

Voith Group
St. Pöltener Str. 43
89522 Heidenheim, GERMANY

Phone: + 49 7951 32 1666
E-mail: Industry.Service@voith.com
Internet: www.voith.com

If you have questions regarding the Voith product, please contact the Voith Service.

3201-014141 en

This document describes the state of design of the product at the time of the editorial deadline.

Installation and Operating Manual / 3201-014141
en / Protection Class 0: public

Contents

1 Possible Applications, Characteristics of the OnSens.SmarTemp

The self-contained non-contacting thermal measuring device (OnSens.SmarTemp) is a monitoring system for Voith turbo couplings.

The system is used to measure the operating medium temperature of Voith turbo couplings of sizes **366 up to 1330** (measuring range: -40 °C to 200 °C).

The non-contacting signal transmission allows measuring the operating medium temperature during active operation and to draw conclusions to the actual coupling stress.

As the temperature is measured directly in the operating medium, changes of stress are quickly identified allowing to quickly react to possible overloads and to prevent excess temperatures.

The loss of coupling filling through the fusible plugs and associated downtimes can reliably be avoided.

Please note that the OnSens.SmarTemp, like any other temperature measuring system, indicates the temperature with some time delay.
For evaluation and further processing of the data in the machine control system, the time delay depending on the actual heating-up velocity of the operating fluid has to be considered.

Moreover, the input power available for machine operation can be optimally used. Please contact Voith.

Benefits and reaction possibilities:

- **Temperature warning**
- **Switch-off of drive motor**
- **Reduction of engine speed (diesel engines)**
- **Reduction of load intake**
- **Optimization of load absorption of driven machine**

Fusible plugs

Fusible plugs
→ Operating manual of turbo coupling

The fusible plugs protect the turbo coupling against damage due to thermal overload.

⚠ WARNING

Risk of personal injuries and damage to property
The turbo coupling will be damaged if operation is continued after a fusible plug responded.

- When the OnSens.SmarTemp is used, it is not allowed to replace the fusible plugs by blind screws or by fusible plugs with different nominal response temperatures.
- Following the shutdown, the control system has to be locked in a way that prevents automatic re-start.
- Switch off the unit in which the turbo coupling is installed and secure the switch against inadvertent switch-on.
- For all work performed on the turbo coupling and OnSens.SmarTemp ensure that both the drive motor and the driven machine have stopped running and that unintended starting is absolutely impossible!
- The coupling may only be restarted if the turbo coupling temperature is below the maximum permissible temperature allowed when switching on the motor!

Maximum allowable temperature
→ Operating manual of turbo coupling

1.1 Use, operation

Intended use
→ Chapter 5.2

The devices are only approved for proper and intended use in accordance with the instructions. Contravention excludes any warranty and responsibility on the part of the manufacturer!

- It is imperative to comply with the ambient conditions as specified in this operating manual.
- The provision of lightning protection measures have to be ensured by the operator.
- Ensure that the fusible plugs required in addition are used on each turbo coupling which is operated with this measuring system.
- Operating the turbo coupling with OnSens.SmarTemp is permissible only with a suitable protective cover.

Fusible plugs
→ Operating manual of turbo coupling

Protective cover
→ Operating manual of turbo coupling

2 OnSens.SmarTemp Functioning

The self-contained non-contacting thermal measuring device (OnSens.SmarTemp) consists of three main components:

- **Temperature sensor (OnSens.SmarTemp sensor)**
- **OnSens.SmarTemp blind screw**
- **Stationary receiver**

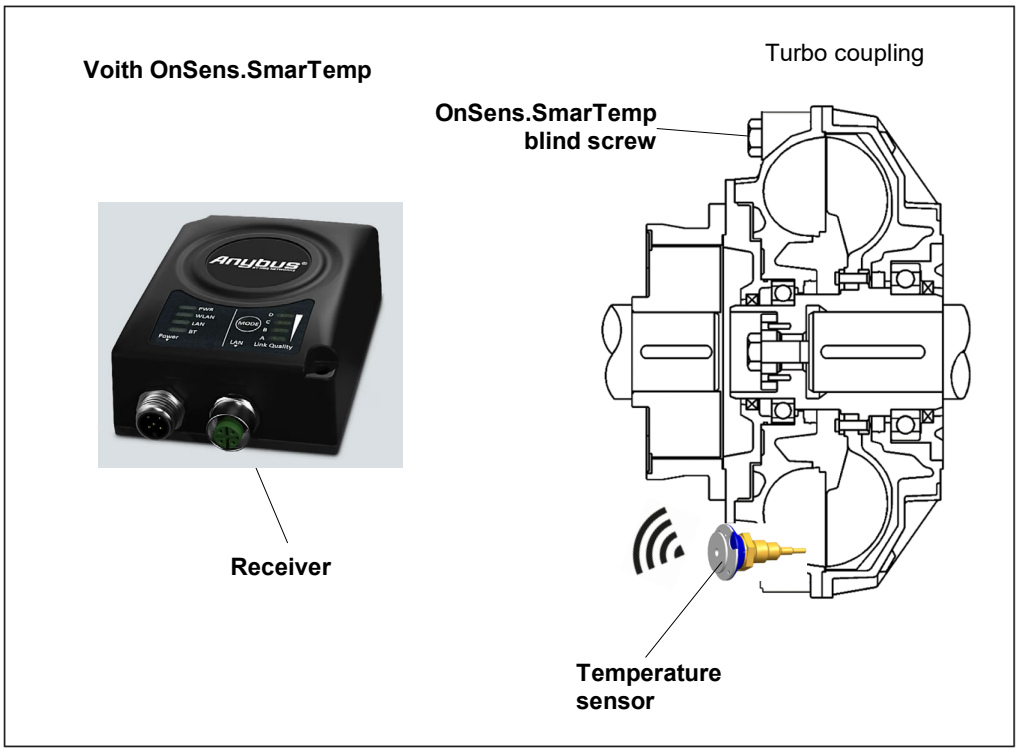


Fig. 1

2.1 Temperature sensor (OnSens.SmarTemp sensor)

The temperature sensor is a self-contained component. It is screwed into the turbo coupling outer wheel and its measuring tip projects directly into the operating medium.

The temperature sensor transmits the measuring signal to the stationary receiver without contact. The range of this signal is dependent on the constructional conditions at the jobsite and is typically at least 10 meters.

To ensure the function of the temperature sensor, the temperature of the operating medium of the coupling must be at least approx. 20 Kelvin higher than the ambient temperature over a longer period during nominal operation uf the unit. If the temperature falls below this temperature difference (e.g. during standstill, no-load operation or operation with low load), the internal power supply is not sufficient and the OnSens.SmarTemp sensor does not transmit a stable continuous signal.

As the temperature sensor is not completely warmed up when the unit is started, it requires a higher temperature difference until a stable temperature signal can be transmitted. The temperature difference required between operating medium of the coupling and ambient temperature is maximally approx. 60 Kelvin in this non-steady operating state.

2.2 OnSens.SmarTemp blind screw

The OnSens.SmarTemp blind screw is provided to compensate the mass of the temperature sensor and it is mandatory to install the same exactly opposite the temperature sensor. Without OnSens.SmarTemp blind screw, impermissible forces will occur due to unbalance which may damage the machine system.

2.3 Stationary receiver

The stationary receiver receives the radio signal from the temperature sensor and transmits it to the unit's control system.

For the receiver function, it must be connected to a power supply (9 ... 30 V DC) with a cable. A data cable is required for data transmission to the machine control system. Both cables are included in the Voith scope of supply.

With a receiver it is possible to receive up to 7 temperature sensors at the same time and without restrictions.

Further information on the receiver can be found in the annex to this operating manual.

3 Technical data

3.1 Temperature sensor

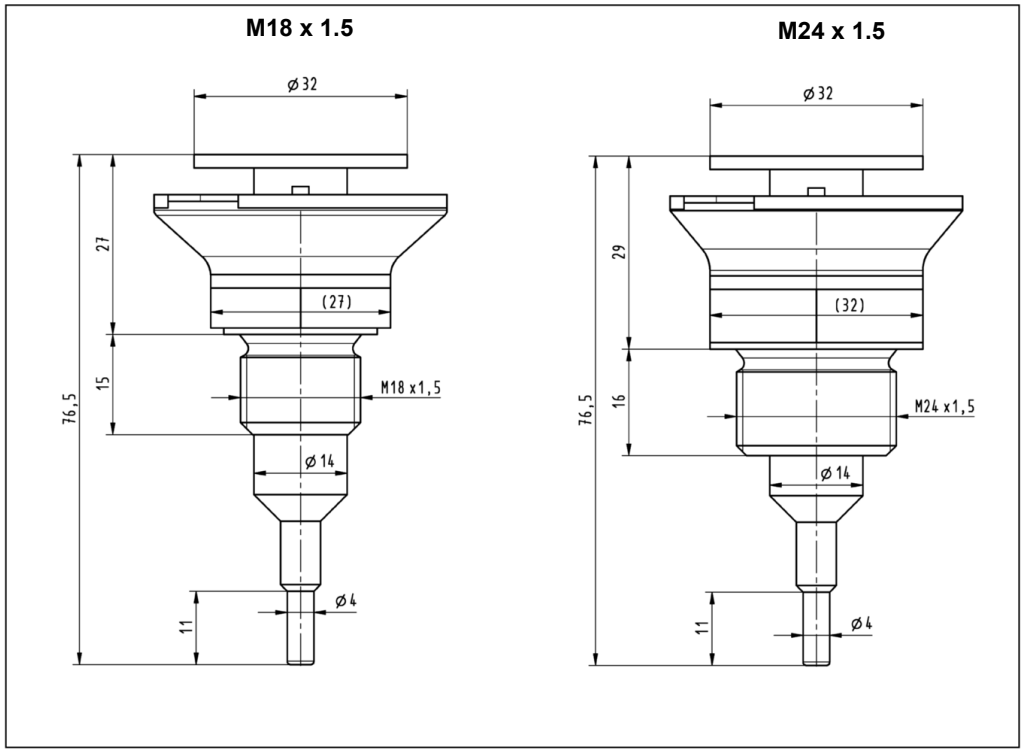


Fig. 2

The following temperature sensors are available for the different turbo coupling sizes.

Dimension of thread	M18x1.5	M24x1.5
Suitable for coupling sizes	366 – 650	750 - 1330
Width across flats	27	32
Tightening torque	50 Nm	144 Nm
Weight	104 ± 2 g	148 ± 2 g
Protection to EN 60529	IP 65	
Measuring range	-40 °C … +200 °C	
Operating medium temperature (temporarily)	max. 200 °C	
Measuring tolerance	± 2 K	
Permissible ambient temperature	-40 °C … 85 °C	
Minimum required temperature difference between the operating medium and the environment	> 20 K	
Signal range (depending on installation condition on the jobsite)	up to 10 m	

Table 1

Like any other temperature measuring system, the temperature sensor has a measuring error which depends on the heating rate of the coupling's operating medium.

Without knowing the drive and turbo coupling design in detail, the following limit temperatures provide a reliable thermal monitoring of the coupling:

1. During nominal operation:

$$\vartheta_{Bmax} = \begin{array}{l} 95\ °C \text{ with NBR seals (Perbunan)} \\ 105\ °C \text{ with FPM seals (Viton)} \end{array}$$

2. Temporarily while the driven machine starts or in case of blocking:

$$\vartheta_{SPmax} = \vartheta_{FP} - 45\ K$$

If more details of the drive and turbo coupling are known, it is possible to optimize these limit temperatures. Please contact Voith.

Symbol	Definition	Unit
ϑ_{Bmax}	Maximum operating temperature (permanently)	°C
ϑ_{SPmax}	Maximum peak temperature (temporarily)	°C
ϑ_{FP}	Nominal response temperature of fusible plugs (see turbo coupling)	°C

3.2 OnSens.SmarTemp blind screws

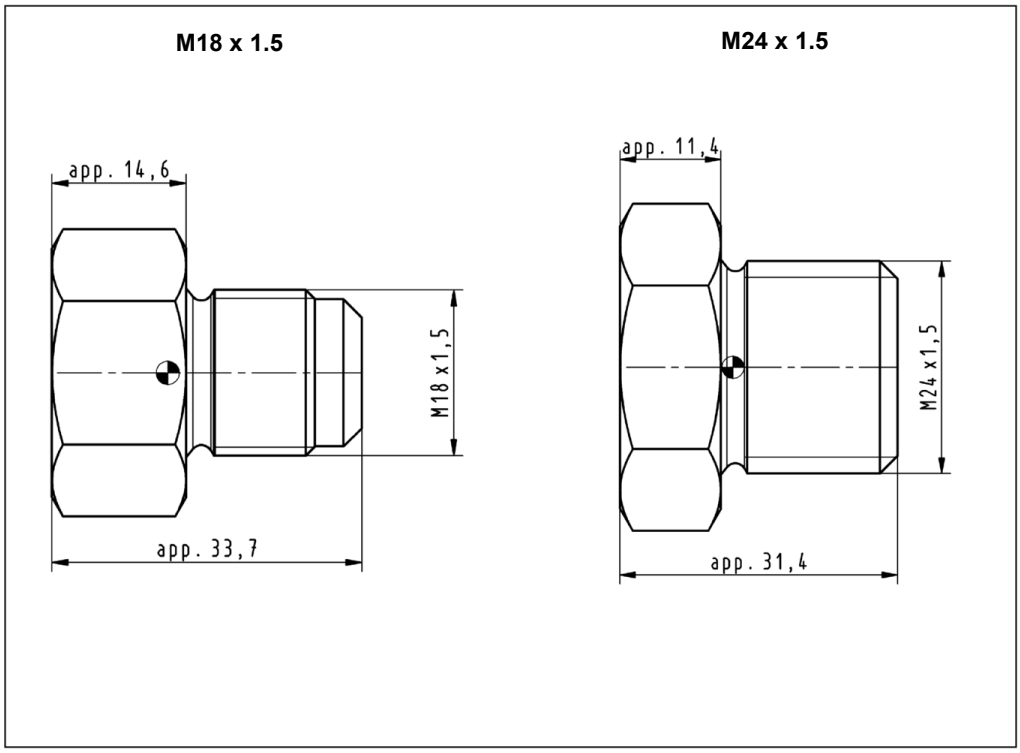


Fig. 3

The following OnSens.SmarTemp blind screws are available for the different turbo coupling sizes:

Dimension of thread	M18x1.5	M24x1.5
Suitable for coupling sizes	366 – 650	750 – 1330
Width across flats	27	32
Tightening torque	50 Nm	144 Nm
Weight	104 ± 2 g	148 ± 2 g

Table 2

3.3 Stationary receiver

Fig. 4

Radio module signal	Receiver and WLAN
Protection to EN 60529	IP 65
Supply voltage range	9 V DC… 30 V DC
Supply current	typ. 54 mA (at 24 V DC)
Current consumption	max. 190 mA (at 9 V DC)
Max. power loss at nominal condition	1.7 W
Type of connection - power supply	M12 plug-in connector (A-coded, male)
Type of connection - Ethernet	M12 plug-in connector (D-coded, female)
Max. number of connectable temperature sensors	7
Permissible ambient temperature (operation)	-30 °C … +65 °C
Permissible humidity (operation)	5 % … 93 % (non-condensing)

Table 3

Further information on the receiver can be found in the annex to this operating manual.

Suitable cables for the power supply and data transmission are included in the Voith scope of supply.

4 User Information

This manual will support you in using the non-contacting thermal measuring device (**OnSens.SmarTemp**) in a safe, proper and economical way.

If you observe the information contained in this manual, you will
- increase the reliability and lifetime of the unit,
- avoid any risks
- reduce repairs and downtimes.

This manual must
- always be available at the OnSens.SmarTemp place of use,
- be read and used by every person who works on the unit or commissions the same.

The non-contacting thermal measuring device (OnSens.SmarTemp) has been manufactured to the latest design standard and approved safety regulations. Nevertheless, the user's or third party's life may be endangered or the unit or other property impaired in case of improper handling or unintended use.

Spare parts:
Spare parts must comply with the technical requirements stipulated by Voith. This is ensured by using original spare parts.
Installation and/or use of non-original spare parts may negatively change the characteristics of the **OnSens.SmarTemp** and may thus impair safety.
Voith is not liable for any damages resulting from the use of non-original spare parts.

Use only appropriate workshop equipment for maintenance. Professional maintenance and/or repair can only be guaranteed by the manufacturer or an authorized specialist workshop.

This manual has been issued with utmost care. However, should you need any further information, please contact:

Voith Group
St. Pöltener Str. 43
89522 Heidenheim, GERMANY

Phone: + 49 7951 32 1666
E-mail: Industry.Service@voith.com
Internet: www.voith.com

Voith reserves the right for modifications.

5 Safety

5.1 Safety information

Safety information indicating the descriptions and symbols as described in the following are used in the operating manual.

5.1.1 Structure of safety information

⚠ DANGER WORD
Consequences of a hazardous situation Source of hazard • Hazard prevention

Danger word
The danger word divides the severity of the danger in several levels:

Danger word	Severity of danger
⚠ DANGER	Death or serious injury (irreversible personal injury)
⚠ WARNING	Death or serious injury possible
⚠ CAUTION	Minor or moderate injury possible
NOTICE	Possibly damage to property of - the product - its environment
i INFORMATION	For useful additional information on proper handling of the product only

Table 4

Consequences of a hazardous situation
Hazard consequences indicate the kind of hazard.

Source of hazard
The source of hazard indicates the cause of hazard.

Hazard prevention
Hazard prevention describes the measures to be taken to prevent a hazard.

5.2 Intended use

- The non-contacting thermal measuring device (OnSens.SmarTemp) serves for the non-contacting temperature monitoring on Voith turbo couplings. Any use beyond that described herein, e.g. for operating or application conditions that have not been agreed upon, is deemed unintended.
- Intended use also includes observing this installation and operating manual.
- The manufacturer is **not** liable for any damages resulting from unintended use. The risk has to be borne solely by the user.

5.3 Unintended use

Design range
→ Operating manual of turbo coupling

- Design range is not met.
- Any use beyond that described herein, e.g. for higher powers, higher speeds or operating conditions that have not been agreed upon, is deemed unintended.
- Moreover, it is not permitted to use OnSens.SmarTemp units from third parties.

5.4 General information as to dangerous situations

For all work performed on the non-contacting thermal measuring device, please observe the local regulations for the prevention of accidents as well as the regulations for installation of electrical equipment!

Hazards while working on the non-contacting thermal measuring device:

⚠ DANGER

Electric shock
On account of incorrectly mounted or incorrectly connected electrical components, and disconnected electric connections, persons could get an electric shock and be severely injured, possibly with fatal consequences.
Incorrectly mounted or incorrectly connected electrical components and disconnected electric connections may cause damages to the machinery.

- A qualified electrician has to properly carry out the connection to the electric supply network considering the system voltage and the maximum power consumption!
- The system voltage has to be in conformity with the system voltage indicated on the nameplate.
- There has to be a corresponding electrical protection by a fuse on the network side.

Electric shock:

DANGER

Electrostatic processes
Electrostatic charging may injure persons by an electric shock.

- Allow only a qualified electrician to install the equipment into which the turbo coupling is installed.
- The unit and the electrical installation are provided with ground connections.

Working on the turbo coupling:

WARNING

Risk of injury
While working on the turbo coupling, there is the risk of injury through cutting, crushing, burns and cold burns in case of minus degrees.

- Please observe the installation and operating manual of the turbo coupling!
- Never touch the turbo coupling without wearing protective gloves.
- Start to work on the turbo coupling only after it has cooled down.
- Ensure that there is sufficient light, a sufficiently large working space and good ventilation when working on the turbo coupling.
- Switch off the unit in which the turbo coupling is installed and secure the switch against inadvertent switch-on.
- For all work performed on the turbo coupling ensure that both the drive motor and the driven machine have stopped running and that unintended starting is absolutely impossible!

Electric welding near the OnSens.SmarTemp:

NOTICE

Damage to property
Damage to electronic components in the temperature sensor and receiver by non-compliance with the specifications.

- Before beginning with welding work close to the OnSens.SmarTemp (5 m distance from temperature sensor or receiver), disconnect all lines from the receiver.

Noise:

Sound pressure level
→ cover sheet of operating manual of turbo coupling

⚠ WARNING

Hearing loss, permanent impairment of hearing
The turbo coupling generates noise during operation. If the A-classified equivalent sound pressure level $L_{PA,\ 1m}$ exceeds 80 dB(A), this may cause impairment of hearing!

- Wear ear protection.

Operating fluid which sprays off or leaks out:

⚠ WARNING

Risk of losing sight due to operating fluid spraying off, risk of burning
In case of thermal overload of the turbo coupling, the fusible plugs respond. Operating fluid leaks out through these fusible plugs.
This may happen only in case of unintended use.

Unintended use
→ Chapter 5.3

- Persons close to the turbo coupling have to wear safety goggles.
- Please make sure that the spraying-off operating fluid cannot get in contact with persons.
- After the fusible plugs have sprayed off, switch off the drive immediately.
- Electrical devices located near the turbo coupling need to be splash-guarded.

⚠ WARNING

Fire hazard
After the fusible plugs responded, spraying off oil may ignite on hot surfaces causing fire, as well as releasing toxic gases and vapor.

- Make sure that spraying off operating fluid cannot get into contact with hot machine parts, heaters, sparks or open flames.
- Immediately switch off the driving machine when the fusible plugs respond.
- Please pay attention to the information contained in the safety data sheets.

⚠ CAUTION

Slipping hazard
Slipping hazard by sprayed off solder of fusible plugs and leaking out operating fluid.

- Please provide a catch pan of sufficient size.
- Immediately remove any leaking out solder and operating fluid.
- Please pay attention to the information contained in the safety data sheets.

Rotating parts or parts flying around:

⚠ WARNING

Risk of personal injuries and damage to property
Rotating parts, such as the turbo coupling itself and exposed shaft parts need to be protected by a protective cover against contact with and entry of loose parts. Moreover, there is a risk of parts flying around in case of a damage to the temperature sensor.

- Never operate the turbo coupling without protective cover.

5.5 Remaining risks

⚠ WARNING

Risk of personal injuries and damage to property
Unintended use or incorrect operation may cause death, serious injuries or minor injuries as well as damage to property and the environment.

- Only persons who are sufficiently qualified, trained and authorized are allowed to work on or with the turbo coupling and the non-contacting thermal measuring device (OnSens.SmarTemp).
- Please observe the warnings and safety information.

5.6 What to do in case of accidents

- In case of accidents, please observe the local regulations, the operating manuals and the operator's safety measures.

5.7 Information with regard to operation

- If irregularities are found during operation, immediately switch off the drive unit.

5.8 Qualification of staff

Only qualified and authorized professional staff are allowed to perform work, such as transportation, storage, installation, electrical connection, commissioning, operation, maintenance, servicing and repair.

Qualified professional staff in the sense of this installation and operating manual are persons who are familiar with transportation, storage, installation, electrical connection, commissioning, maintenance, service and repair, and who have the necessary qualifications for their job. Qualification has to be ensured by performing training and giving instructions.

This staff must be trained, instructed and authorized to:
- operate and service machines in a professional manner in accordance with the technical safety standards.
- use lifting appliances, slings (ropes, chains, etc.) and lifting points in a professional manner.
- properly dispose of media and their components, e.g. lubricating grease.
- service and use safety devices in a manner that ensures compliance with safety standards.
- prevent accidents and provide first aid.

Staff to be trained may only perform work on the turbo coupling and the non-contacting thermal measuring device (OnSens.SmarTemp) under the supervision of a qualified and authorized person.

The staff in charge of any work to be done on the non-contacting thermal measuring device (OnSens.SmarTemp) must
- be reliable,
- have the legal age,
- be trained, instructed and authorized with regard to the intended work.

5.9 Product monitoring

We are under legal obligation to keep the performance of our products under observation, even after shipment.
Therefore, please inform us about anything that might be of interest to us. For example:
- Change in operating data,
- experience gained with the machine,
- recurring problems,
- problems experienced with this installation and operating manual.

For our address,
→ **Page 2**

6 Installation

⚠ WARNING

Risk of injury
Please observe, in particular, → Chapter 5 (Safety) when working on the non-contacting thermal measuring device (OnSens.SmarTemp!

- Before beginning with the installation, ensure that an isolation of all components is guaranteed.
- The fusible plugs protect the turbo coupling against damage due to thermal overload.
  Even when the OnSens.SmarTemp is used, it is not allowed to replace the fusible plugs by blind screws or by fusible plugs with different nominal response temperatures!
- Never operate the turbo coupling without fusible plugs!
- After fitting the temperature sensor, it is mandatory to re-mount the protective cover around the turbo coupling!

6.1 As delivered condition, scope of supply

- Temperature sensor (OnSens.SmarTemp) with sealing ring
- OnSens.SmarTemp blind screw (counterweight) with sealing ring
- Stationary receiver
- Cable for power supply, length: 5 meters
- Network cable, length: 5 meters

In case of a subsequent installation of an OnSens.SmarTemp into the following turbo coupling sizes, please contact Voith Turbo:

Coupling size	Date of manufacture
487	until 2007-06
562	until 2007-06
650	until 2006-08
1000	until 2005-06

Table 5

6.2 Mounting the temperature sensor (OnSens.SmarTemp sensor)

NOTICE

Damage to property
Non-compliance with mounting instructions.
- In order to avoid any damages, mount the temperature sensor after installation of and before filling the turbo coupling.
- Observe the tightening torque for temperature sensors (→ Chapter 3.1).

- Documentation of the MAC addresses of all temperature sensors mounted. This address is engraved on the outside of the temperature sensor (12-digit, format: xx-xx-xx-xx-xx-xx).
- Replace the blind screw by the temperature sensor with the sealing ring in the turbo coupling outer wheel (item 0300) [1]. For tightening torque, see → Chapter 3.1.

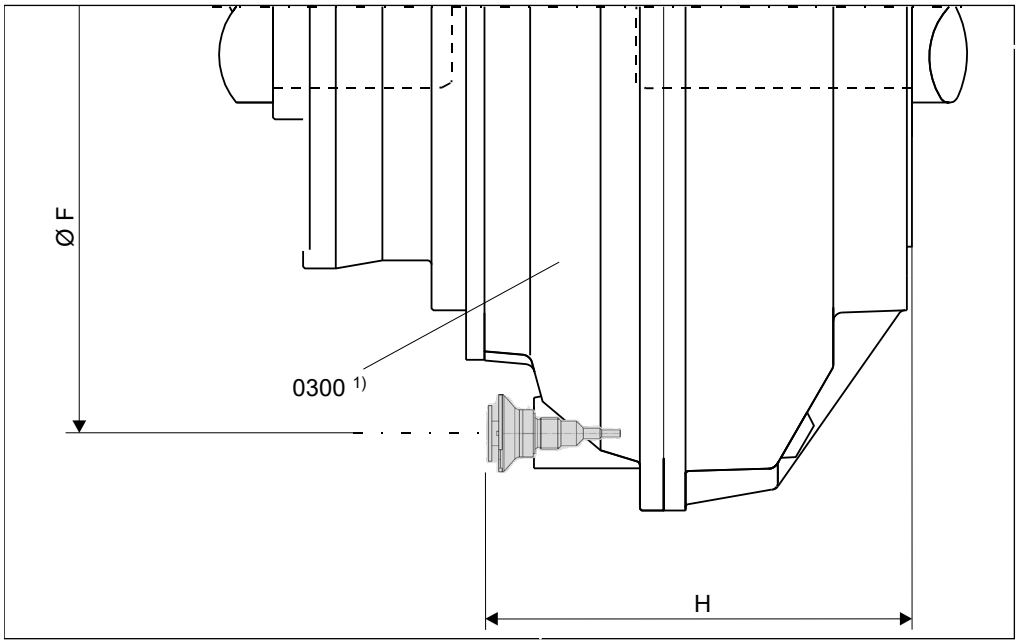


Fig. 5

1) For turbo couplings of type DT, installation is also possible on the opposite outer wheel side.

Installation dimensions for temperature sensor (OnSens.SmarTemp sensor):

	Outer wheel side	
Turbo coupling type	**Pitch circle diameter Ø F [mm]**	**Distance ~ H [mm]**
366 T	350 ± 1	196.5
422 T	396 ± 1	209.5
487 T	470 ± 1	231.5
562 T	548 ± 1	251.5
650 T	630 ± 1	292.5
750 T	729 ± 1	322
866 T	840 ± 1	360
866 DT	840 ± 1	604
1000 T	972 ± 1	373
1000 DT	972 ± 1	676
1150 T	1128 ± 1	462
1150 DT	1128 ± 1	787
1330 DT	1302 ± 1	916

Table 6

Please see the assembly plan of the turbo coupling for installation dimensions of deviating arrangements.

6.3 Mounting the OnSens.SmarTemp blind screw

⚠ WARNING

Risk of personal injuries and damage to property
Impermissible unbalance.
- Always use an OnSens.SmarTemp blind screw.

- Replace the opposite coupling blind screw by an OnSens.SmarTemp blind screw with sealing ring. For tightening torque, see → Chapter 3.1.

6.4 Mounting, connecting the receiver

NOTICE

Damage to property
Non-compliance with mounting instructions.
- Ensure that the fixing for the receiver is of sufficient stability (not included in Voith's scope of supply)!

Damage to the system by electric components not connected properly.
- Use of the two connecting cables included in the scope of supply for power supply and data transmission.
- Consideration of the permissible voltage for the receiver (9 V DC…30 V DC).

- Fix the receiver to a suitable place where the connecting lines and the receiver are protected against damage and direct solar radiation.
- If possible, do not shield the receiver with metal (e.g. by installing it into a closed cabinet) to ensure a stable data transmission.
- Consider a maximum distance of about 10 meters to all temperature sensors to be connected as the range of the signal is limited.
- Lay the data cable contained in the scope of supply to the unit control system.
- Lay the cable contained in the scope of supply to the voltage source (9 V DC…30 V DC, voltage source is not included in the Voith scope of supply). The brown wire corresponds to the positive pole, the blue wire to the negative pole.

7 Integrating the receiver into the unit control system

The temperature sensor sends a temperature signal to the receiver which transmits it to the unit control system. In order to receive this temperature control system, the receiver must be integrated into the superordinate unit control system using the Voith function module as described in the following.

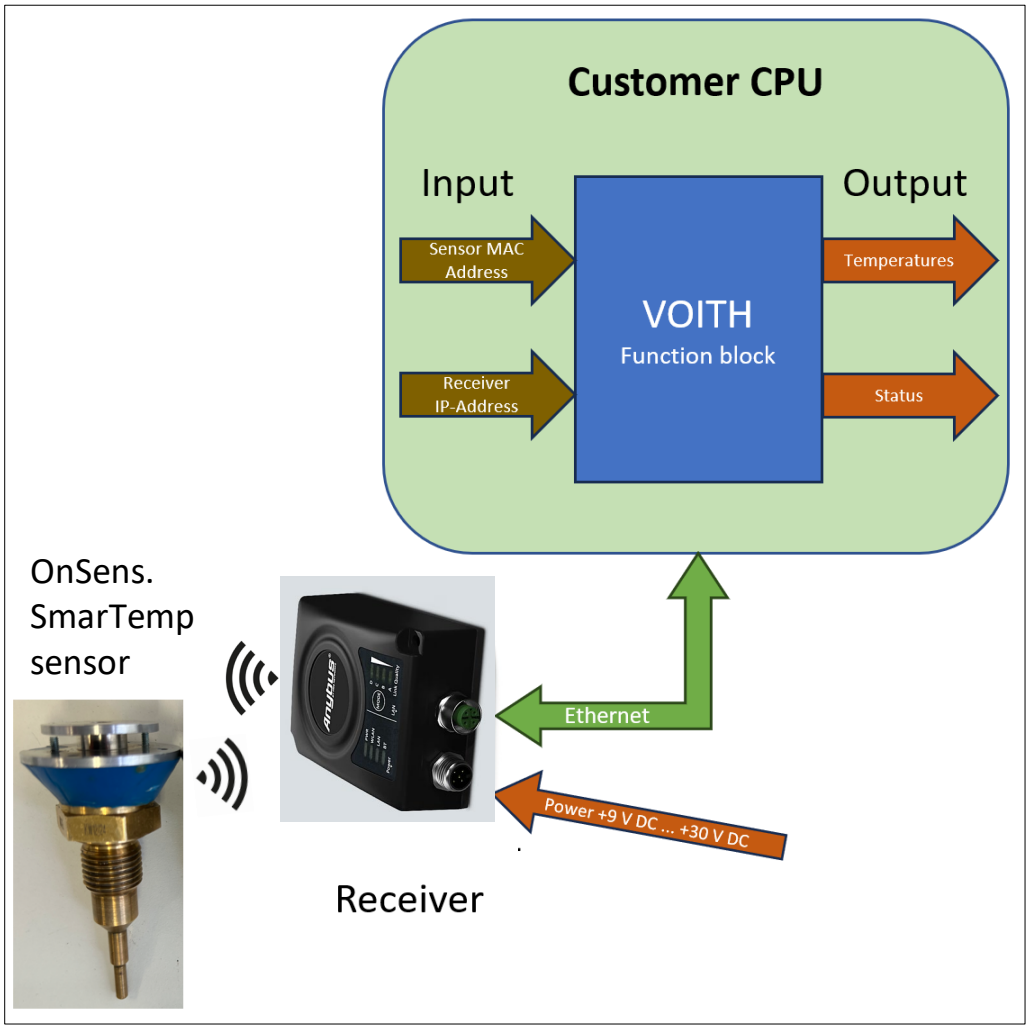


Fig. 6

When using the temperature signal to switch off the unit, the thermal response delay of the temperature sensor must be considered, see → Chapter 3.1.

To integrate the temperature sensors (OnSens.SmarTemp sensors) into the superordinate unit control system, the sensor-specific MAC address is required for each sensor to be integrated. This 12-digit MAC address (format: xx-xx-xx-xx-xx-xx) is engraved on every sensor. Please keep at hand all MAC addresses of the sensors to be integrated.

⚠ WARNING

Risk of personal injuries and damage to property
Inclusion of the receiver in the customer's network

- If the receiver is not connected directly to the unit control system with the supplied network cable, but the signal is transmitted via the customer network, Voith does not assume any safety responsibility for this data transmission.
- In such a case, the customer is responsible for the safety and stability of his network.

7.1 Configuration of receiver

7.1.1 HMS receiver

The receiver is supplied with the factory setting. The IP address of the receiver in factory setting is 192.168.0.99. If necessary, this address must be changed to the desired IP address in advance with any PC. Further information on the receiver can be found in the annex to this operating manual.

7.1.2 Setting the IP address

The receiver must be supplied with power and connected to any PC via Ethernet cable. The PC must be in the same IP range as the receiver. Using a standard browser (e.g. Microsoft Edge), you can call up the web-based management by entering the receiver IP address in the browser. (Factory setting: 192.168.0.99)

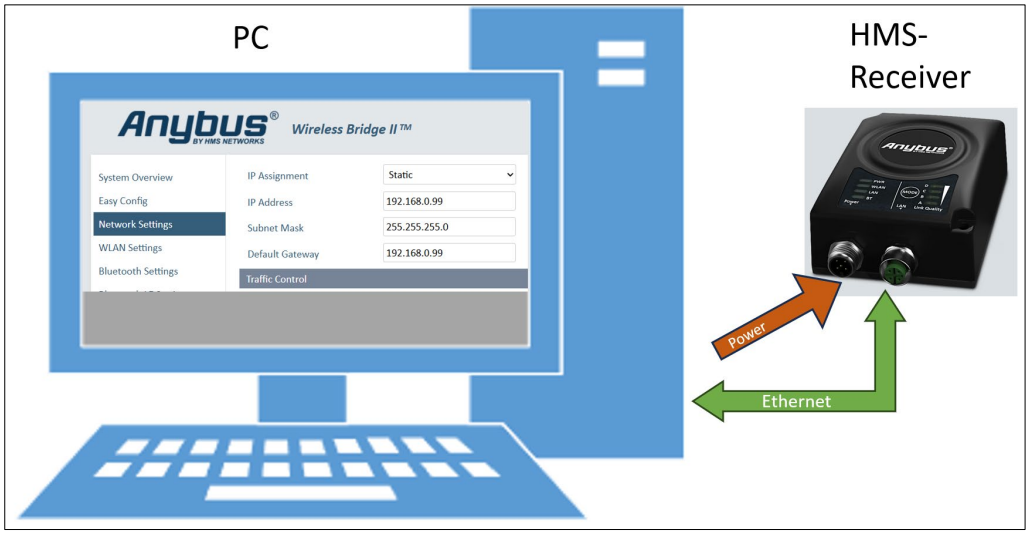


Fig. 7

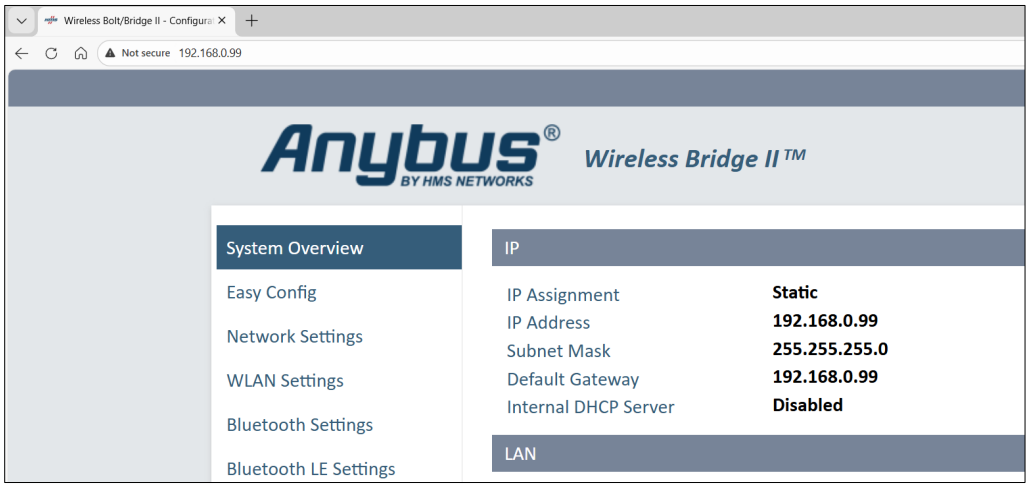


Fig. 8

Go to "Network Settings"

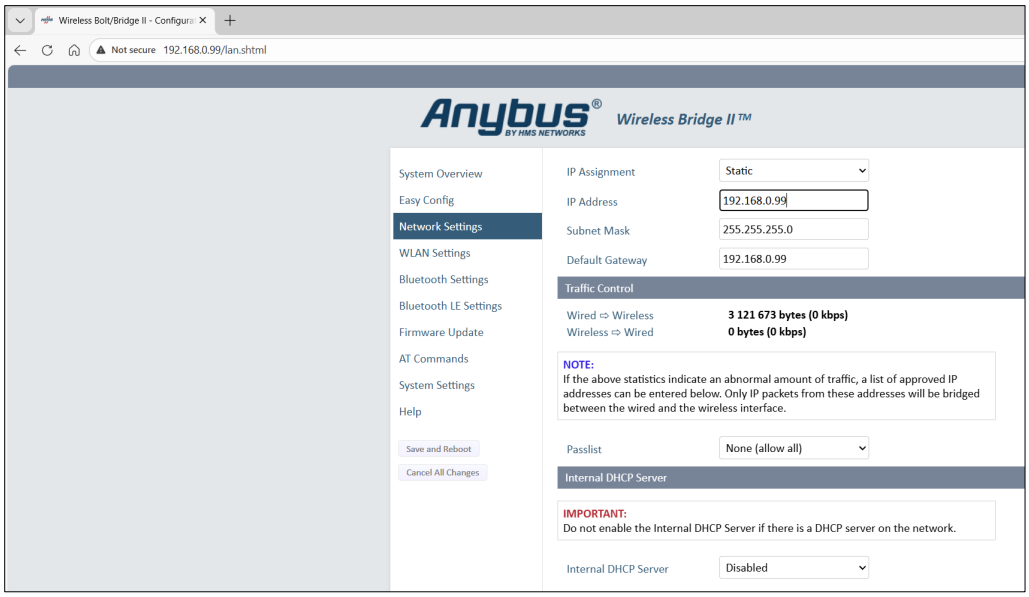


Fig. 9

Then enter the desired IP address, e.g. 192.168.0.251 instead of 192.168.0.99.

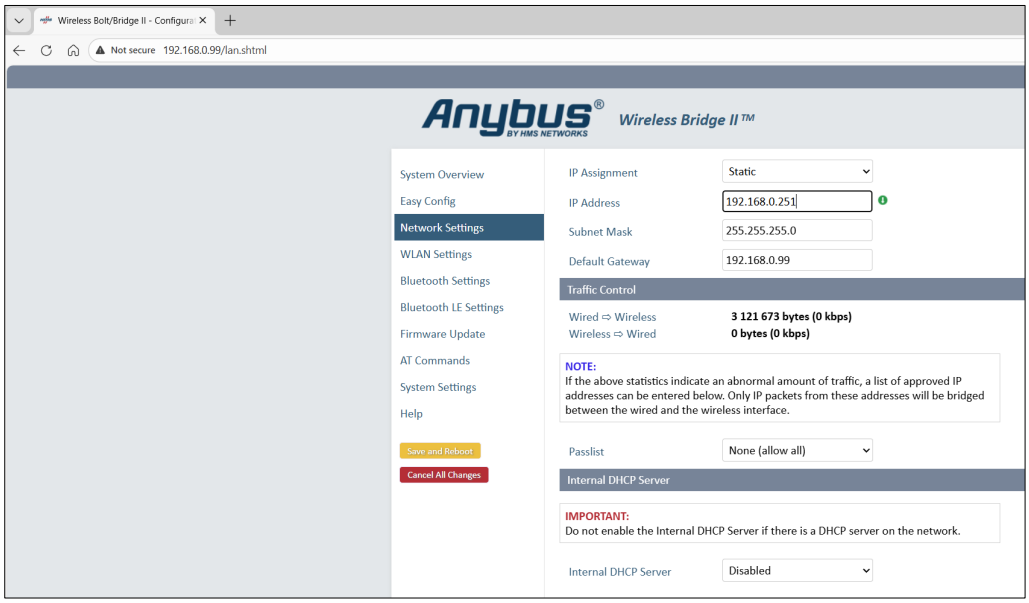


Fig. 10

Then press the "Save and Reboot" button.

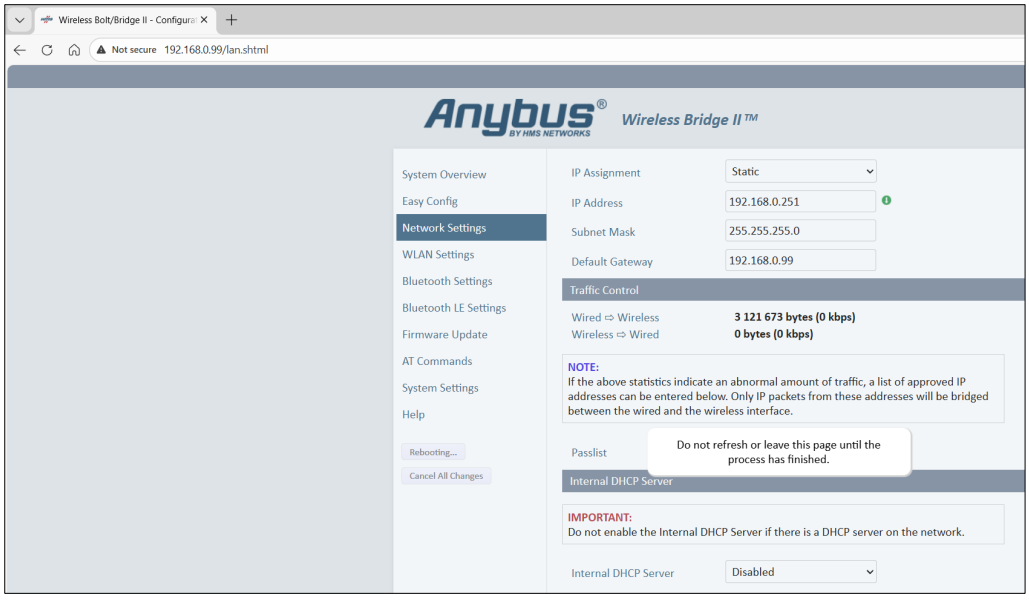


Fig. 11

After a few seconds, the configuration page is automatically updated with the new IP address.

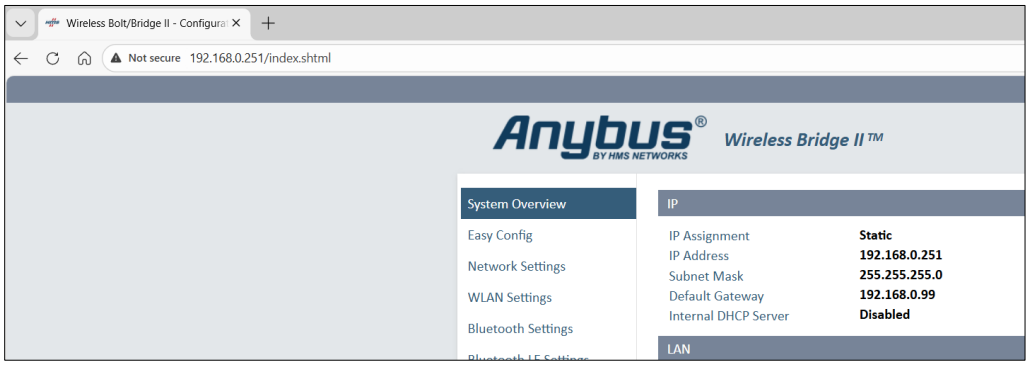


Fig. 12

7.1.3 Resetting the IP address

If the IP address of the receiver is no longer known, the receiver can be reset to the factory settings. The receiver must be supplied with power. After the receiver has started completely (about 10 seconds after switching on), press the MODE button for more than 10 seconds and then release it. The receiver's IP address is set to 192.168.0.99.

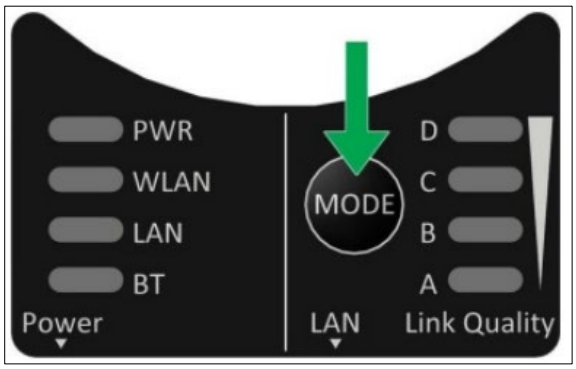


Fig. 13

7.1.4 Password

The user interface offers the option of protecting the receiver with a password (factory setting: no password protection).
However, as the password protection affects the communication with the superordinate function block, the receiver must not be protected with a password.

As the receiver only communicates via the superordinate control unit, the password protection is not necessary.

7.2 Siemens CPU

Function block "FB20_BTM_Ablauf_Sensor_V4" was created for the communication with the receiver (HMS). Up to seven OnSens.SmarTemp sensors can communicate with this receiver.

This chapter applies only to the Siemens CPU S7-1500 control system.
Information required for the integration into a control system of type Allen-Bradley (Rockwell) CPU can be found in Chapter 7.3.
If you are using a different control system, please contact Voith as the function block is not readily compatible with other control models.

The function block was created for the ITA portal, version 17.
If versions higher than version 17 are used, the function block must be upgraded. This upgrading can possibly be carried out directly when opening the library in the TIA portal.
If versions lower than version 17 are used, please consult Voith as the function block is not readily compatible with lower TIA portal versions.

Function block "FB20_BTM_Ablauf_Sensor_V4" is made available together with the operating manual. In case of problems with the provision or integration of the function block, please contact Voith.

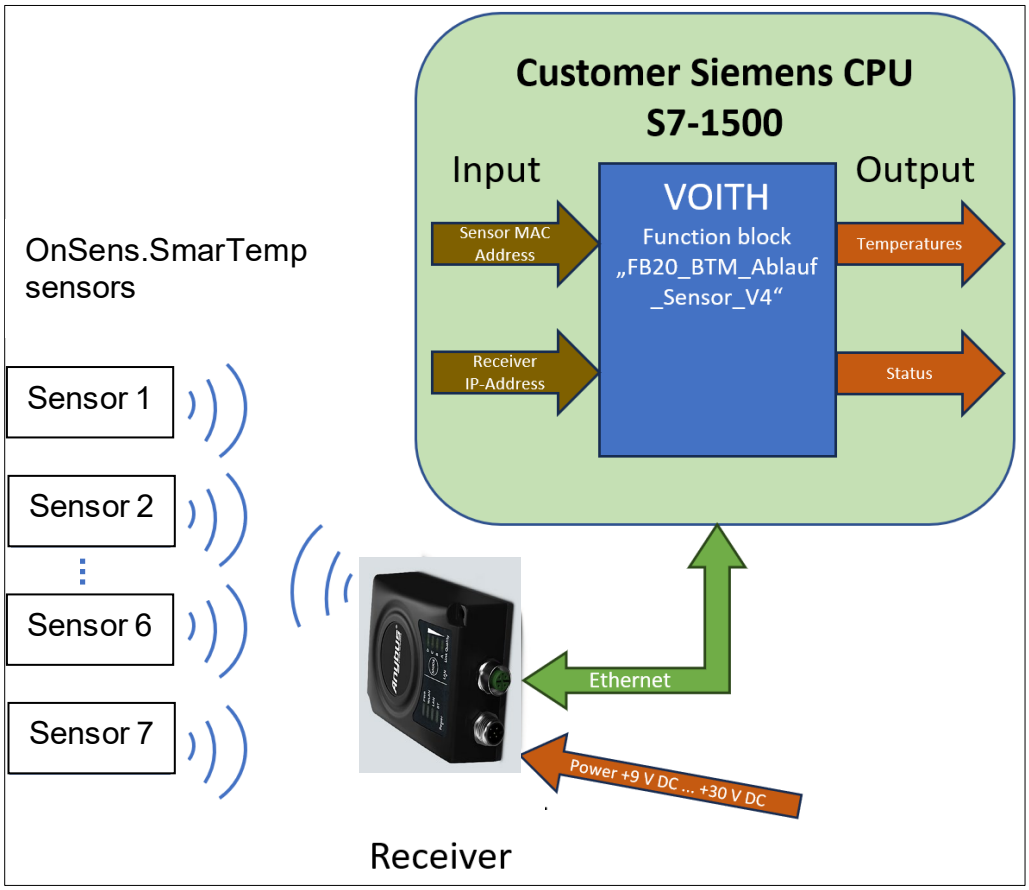


Fig. 14

7.2.1 Setting the CPU

In the CPU, the minimum cycle time should be set to 10 ms. All other CPU settings can be freely parameterized.

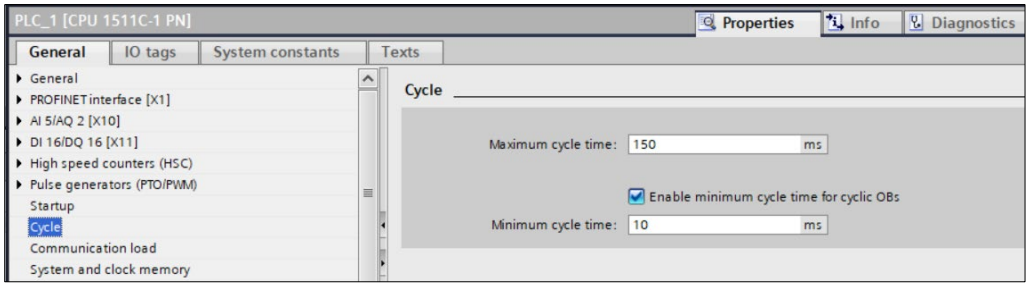


Fig. 15

7.2.2 Using the OnSens.SmarTemp Voith library

Voith provides the necessary global library "BTM-Light_V4.1_xxxx-xx-xx" for controlling the receiver. This was created with the TIA Portal V17.

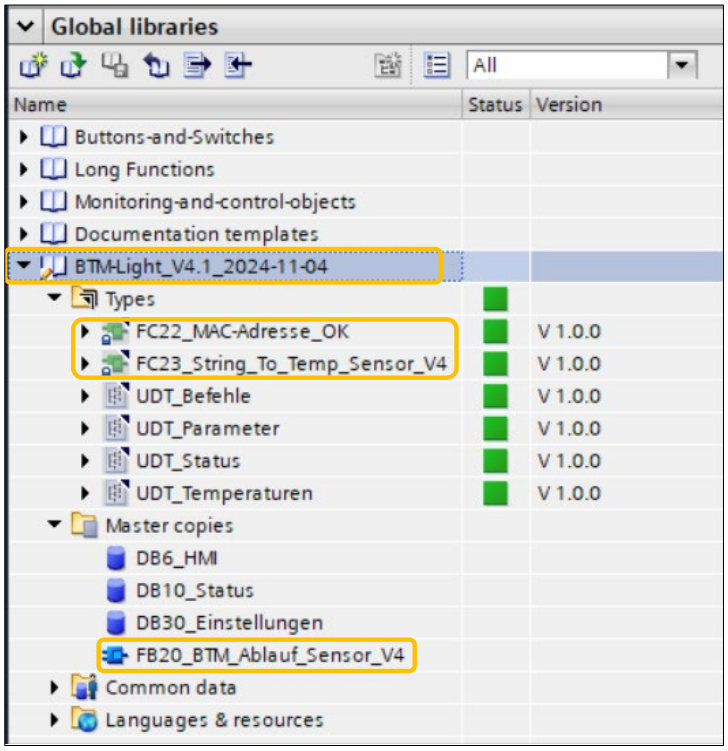


Fig. 16

Functions "FC22_MAC-Adresse_OK" and "FC23_String_To_Temp_Sensor_V4", and function block "FB20_BTM_Ablauf_Sensor_V4" are protected by know-how (Copyright Voith).

7.2.2.1 Opening the archived global library in the TIA portal system project

1. Open the unit project.
2. Click on button "Global library" under "Global Libraries".

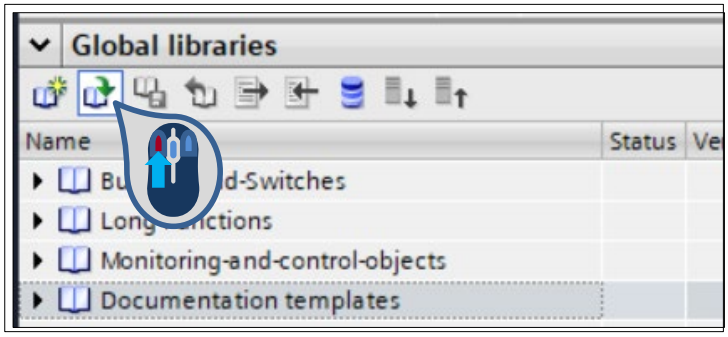


Fig. 17

3. Select "Compressed libraries" from the "File type" drop-down menu. Navigate to the archived "BTM-Light_V4.1_xxxx-xx-xx.zal17" and click on "Open".

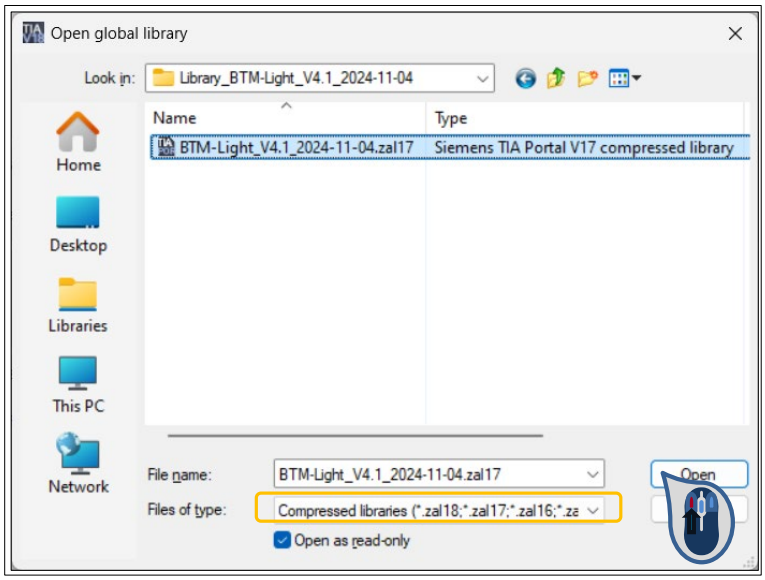


Fig. 18

4. Select the storage path for the de-archived "BTM-Light Library" and acknowledge the dialog with "OK". The de-archived "BTM-Light Library" is opened automatically.
5. If you a using a newer version of TIA Portal, this library will be upgraded to the new TIA Portal version. Here, e.g. from Version V17 to Version V18.

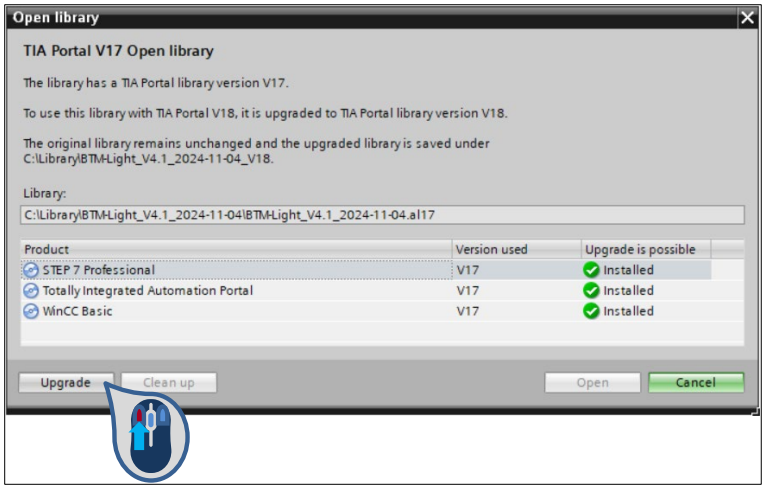


Fig. 19

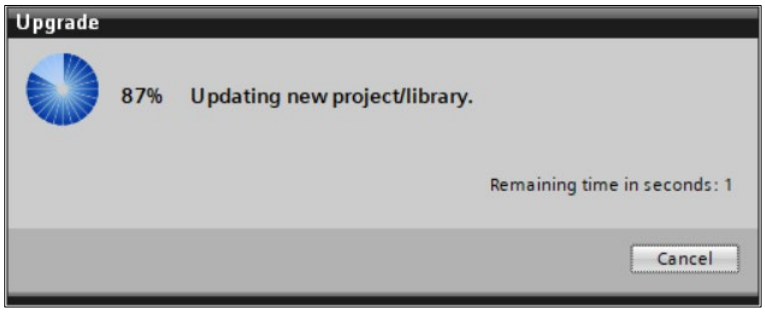


Fig. 20

6. Then the library is opened in TIA Portal Version V18.

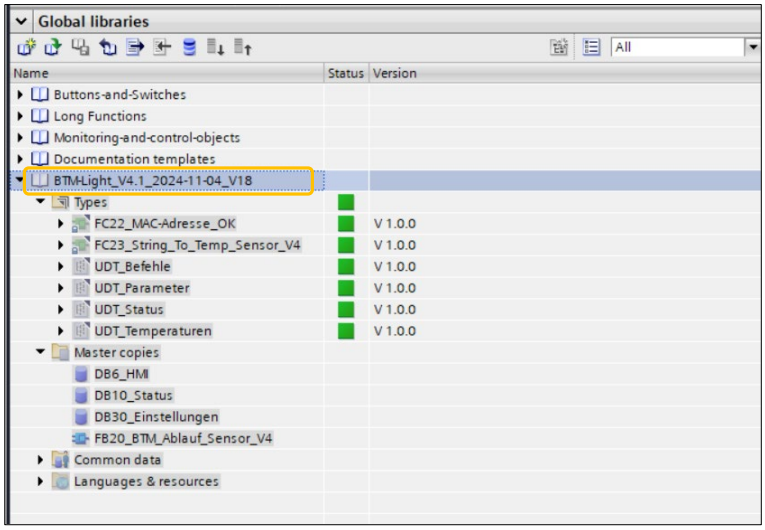


Fig. 21

7.2.2.2 Inserting library elements into the unit project

1. Open your unit project and the global library "BTM-Light_4.1_xxxx-xx-xx".
2. Drag and drop the library elements (FC, FB and DB) into the "Program blocks" folder and the UDT library elements into the "PLC data types" folder.

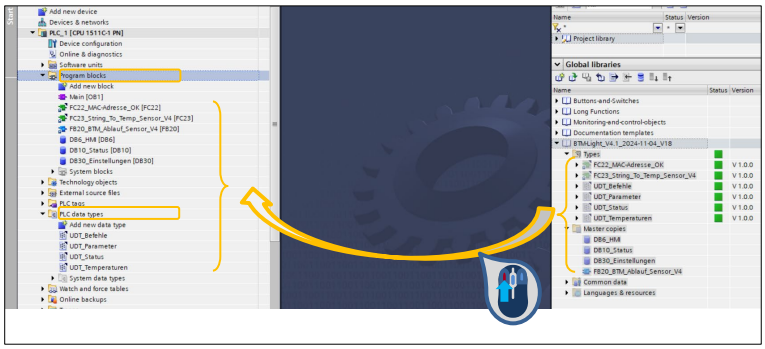


Fig. 22

3. Add the function block "FB20_BTM_Ablauf_Sensor_V4" by drag and drop into the network of the organization block "OB1". An instance data block is created automatically. Enter the name and number of the instance data block and click on "OK".

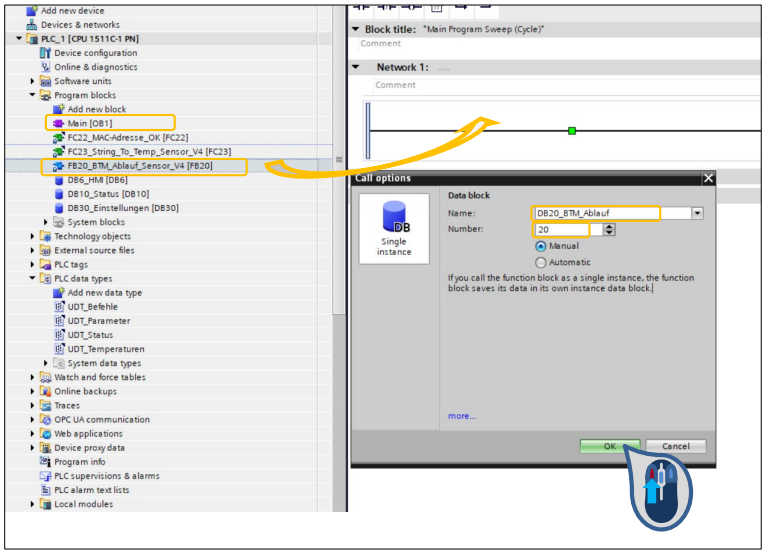


Fig. 23

4. The instance of the function block "FB20_BTM_Ablauf_Sensor_V4" is now displayed in the "OB1" network and the instance data block is displayed in the "Program blocks" folder.

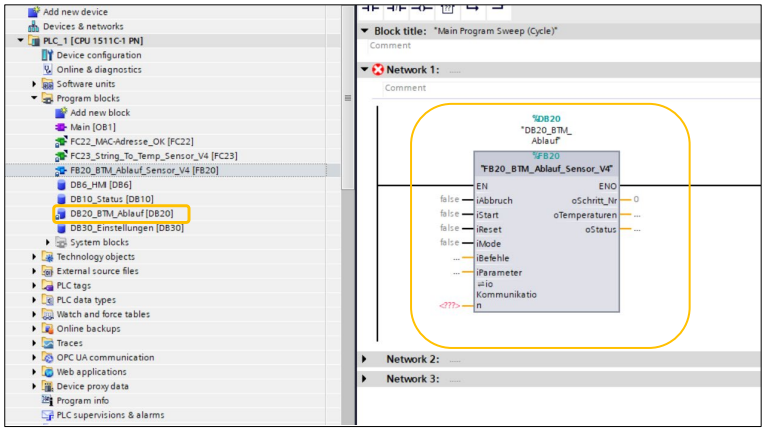


Fig. 24

5. Connect the function block "FB20_BTM_Ablauf_Sensor_V4" as shown here (using drag and drop).

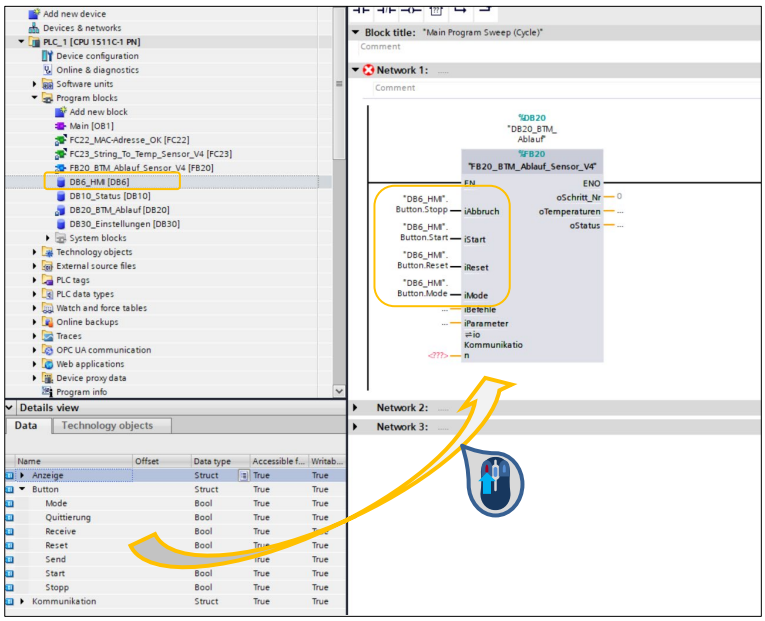


Fig. 25

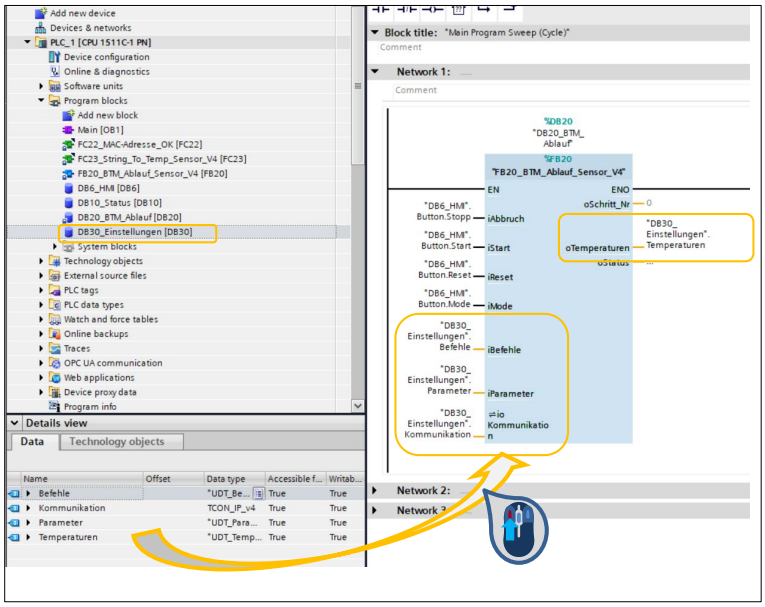

Add new device
Devices & networks
PLC_1 [CPU 1511C-1 PN]
Device configuration
Online & diagnostics
Software units
Program blocks
Add new block
Main [OB1]
FC22_MAC-Adresse_OK [FC22]
FC23_String_To_Temp_Sensor_V4 [FC23]
FB20_BTM_Ablauf_Sensor_V4 [FB20]
DB6_HMI [DB6]
DB10_Status [DB10]
DB20_BTM_Ablauf [DB20]
DB30_Einstellungen [DB30]
System blocks
Technology objects
External source files
PLC tags
PLC data types
Watch and force tables
Online backups
Traces
OPC UA communication
Web applications
Device proxy data
Program info
Details view
Data
Technology objects
Name
Offset
Data type
Accessible f...
Writab...
Befehle
Kommunikation
Parameter
Temperaturen
Block title: "Main Program Sweep (Cycle)"
Comment
Network 1:
Comment
%DB20
"DB20_BTM_
Ablauf"
%FB20
"FB20_BTM_Ablauf_Sensor_V4"
EN
ENO
"DB6_HMI".
Button.Stopp
iAbbruch
oSchritt_Nr
"DB6_HMI".
Button.Start
iStart
oTemperaturen
"DB30_
Einstellungen".
Temperaturen
"DB6_HMI".
Button.Reset
iReset
"DB6_HMI".
Button.Mode
iMode
"DB30_
Einstellungen".
Befehle
iBefehle
"DB30_
Einstellungen".
Parameter
iParameter
"DB30_
Einstellungen".
Kommunikation
Network 2:
Network 3:

Fig. 26

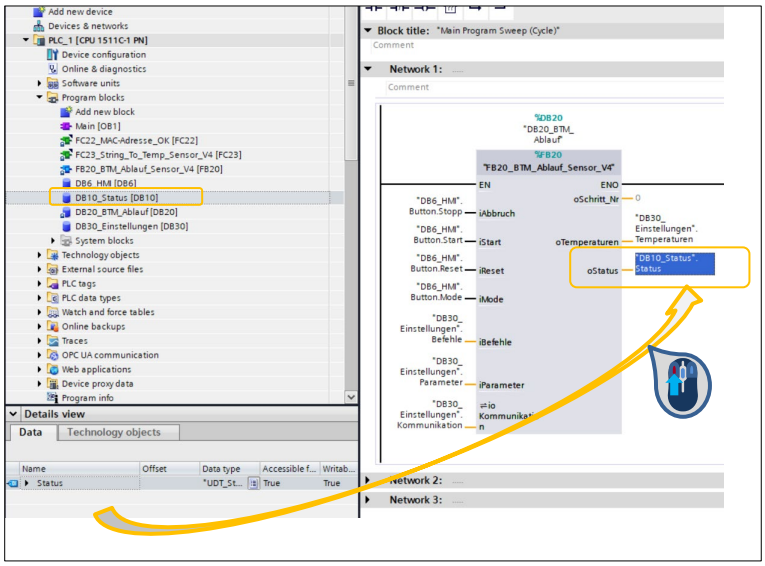

Add new device
Devices & networks
PLC_1 [CPU 1511C-1 PN]
Device configuration
Online & diagnostics
Software units
Program blocks
Add new block
Main [OB1]
FC22_MAC-Adresse_OK [FC22]
FC23_String_To_Temp_Sensor_V4 [FC23]
FB20_BTM_Ablauf_Sensor_V4 [FB20]
DB6_HMI [DB6]
DB10_Status [DB10]
DB20_BTM_Ablauf [DB20]
DB30_Einstellungen [DB30]
System blocks
Technology objects
External source files
PLC tags
PLC data types
Watch and force tables
Online backups
Traces
OPC UA communication
Web applications
Device proxy data
Program info
Details view
Data
Technology objects
Name
Offset
Data type
Accessible f...
Writab...
Status
Block title: "Main Program Sweep (Cycle)"
Comment
Network 1:
Comment
%DB20
"DB20_BTM_
Ablauf"
%FB20
"FB20_BTM_Ablauf_Sensor_V4"
EN
ENO
"DB6_HMI".
Button.Stopp
iAbbruch
oSchritt_Nr
"DB6_HMI".
Button.Start
iStart
oTemperaturen
"DB30_
Einstellungen".
Temperaturen
"DB6_HMI".
Button.Reset
iReset
oStatus
"DB10_Status".
Status
"DB6_HMI".
Button.Mode
iMode
"DB30_
Einstellungen".
Befehle
iBefehle
"DB30_
Einstellungen".
Parameter
iParameter
"DB30_
Einstellungen".
Network 2:
Network 3:

Fig. 27

7.2.3 Description of function block "FB20_BTM_Ablauf_Sensor_V4"

Function block "FB20_BTM_Ablauf_Sensor_V4" is shown on the following picture. This block should be called cyclically in "OB1".

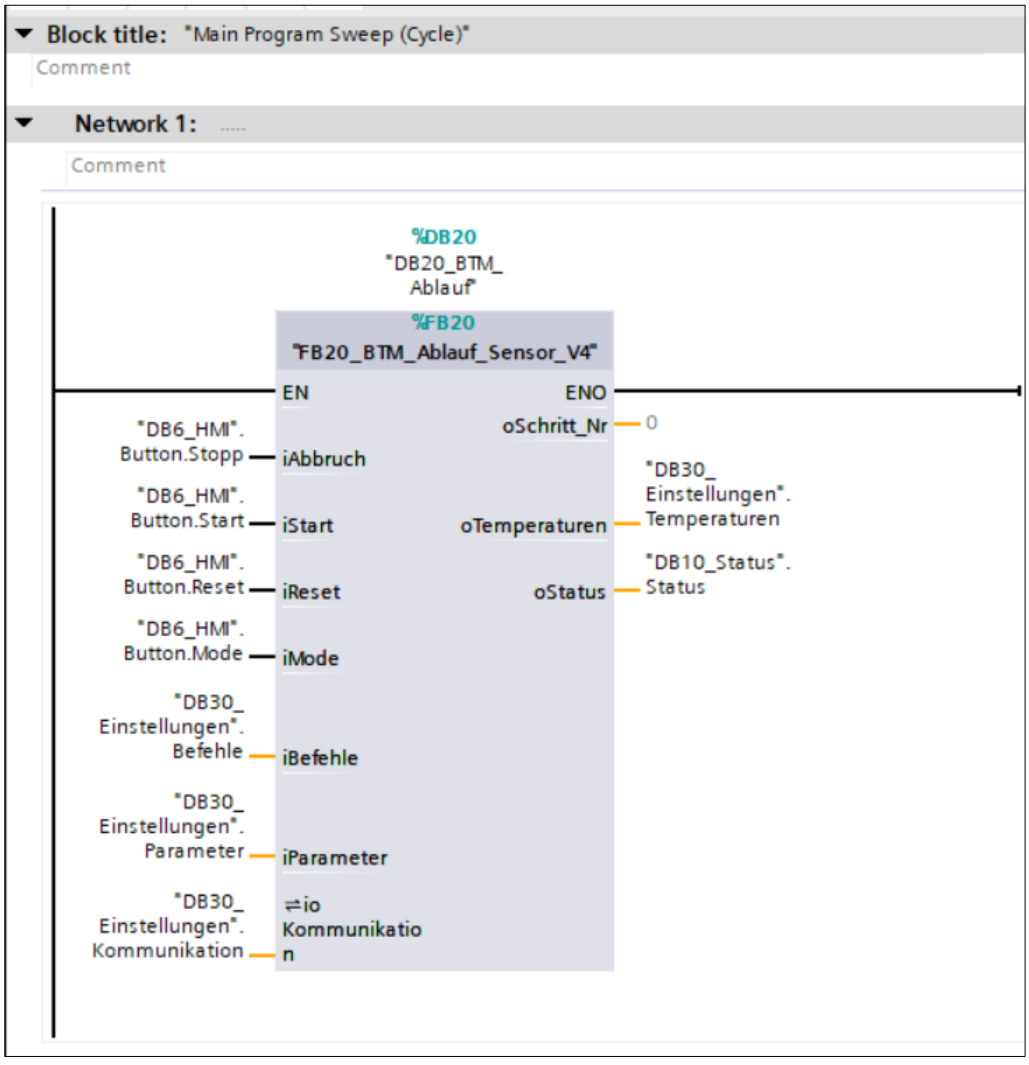


Fig. 28

7.2.3.1 iAbbruch parameter

The iAbbruch parameter is declared as an input and is of the "BOOL" data type. The step chain is aborted or terminated with a positive edge.

7.2.3.2 iStart parameter

The iStart parameter is declared as an input and is of the "BOOL" data type. The step chain is started with a positive edge.

7.2.3.3 iReset parameter

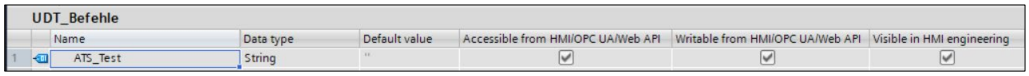
The iReset parameter is declared as an input and is of the "BOOL" data type. With a positive edge, the existing connection of the internal blocks "TSEND_C" and "TRCV_C is reset.

7.2.3.4 iMode parameter

The iMode parameter is declared as an input and is of the "BOOL" data type. If the value of the parameter is "0", automatic mode is preselected. If the parameter has value "1", automatic mode is deactivated and the user can send individual commands to the receiver in test mode.

7.2.3.5 iBefehle parameter

The iBefehle parameter is declared as an input and is of the application-specific "UDT_Befehle" type. It is provided for the test mode so that the user can send individual register commands to the receiver.



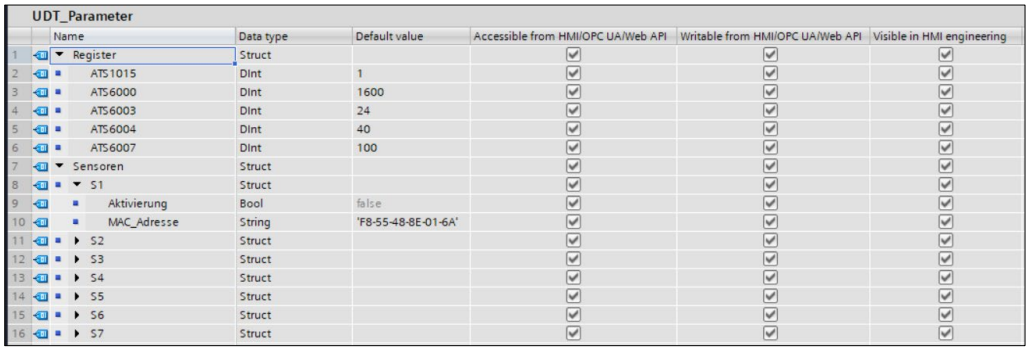
UDT_Befehle

	Name	Data type	Default value	Accessible from HMI/OPC UA/Web API	Writable from HMI/OPC UA/Web API	Visible in HMI engineering
1	ATS_Test	String	''	☑	☑	☑

Fig. 29

7.2.3.6 iParameter parameter

The iParameter parameter is declared as an input and is of the application-specific "UDT_Parameter" type.



UDT_Parameter

	Name	Data type	Default value	Accessible from HMI/OPC UA/Web API	Writable from HMI/OPC UA/Web API	Visible in HMI engineering
1	Register	Struct		☑	☑	☑
2	ATS1015	DInt	1	☑	☑	☑
3	ATS6000	DInt	1600	☑	☑	☑
4	ATS6003	DInt	24	☑	☑	☑
5	ATS6004	DInt	40	☑	☑	☑
6	ATS6007	DInt	100	☑	☑	☑
7	Sensoren	Struct		☑	☑	☑
8	S1	Struct		☑	☑	☑
9	Aktivierung	Bool	false	☑	☑	☑
10	MAC_Adresse	String	'F8-55-48-8E-01-6A'	☑	☑	☑
11	S2	Struct		☑	☑	☑
12	S3	Struct		☑	☑	☑
13	S4	Struct		☑	☑	☑
14	S5	Struct		☑	☑	☑
15	S6	Struct		☑	☑	☑
16	S7	Struct		☑	☑	☑

Fig. 30

The following parameters can be adapted:

- Register parameters (should only be changed by trained qualified staff!):
  - ATS1015: Radio Mode Receiver
  - ATS6000: Advertising Interval Minimum
  - ATS6003: Connect Connection Interval Minimum
  - ATS6004: Connect Connection Interval Maximum
  - ATS6007: Connect Create Connection Timeout
- Sensor parameters:
  - Activation of Sensor x
  - MAC address for Sensor x

Note: The parameters may only be changed when the step chain is switched off!

7.2.3.7 ioKommunikation parameter

The ioKommunikation parameter is declared as InOut and is of type "TCON_IP_v4".

DB30_Einstellungen

	Name	Data type	Start value	Retain	Accessible f...	Writa...	Visible in ...	Setpoint
1	Static							
2	Befehle	"UDT_Befehle"						
3	ATS_Test	String	''					
4	Kommunikation	TCON_IP_v4						
5	InterfaceId	HW_ANY	64					
6	ID	CONN_OUC	16#0001					
7	ConnectionType	Byte	16#0B					
8	ActiveEstablished	Bool	TRUE					
9	RemoteAddress	IP_V4						
10	ADDR	Array[1..4] of Byte						
11	ADDR[1]	Byte	192					
12	ADDR[2]	Byte	168					
13	ADDR[3]	Byte	0					
14	ADDR[4]	Byte	254					
15	RemotePort	UInt	8080					
16	LocalPort	UInt	2001					
17	Parameter	"UDT_Parameter"						
18	Register	Struct						
19	Sensoren	Struct						
20	Temperaturen	"UDT_Temperaturen"						

Fig. 31

The only parameter that can be changed by the user is the remote address (IP address of the receiver). All other parameters must not be changed.
Note: If the IP address is changed, a new start of the CPU is necessary!

7.2.3.8 oSchritt_Nr parameter

The oSchritt_Nr parameter is declared as output, of data type "Integer" and outputs the current step number of the process.

7.2.3.9 oTemperaturen parameter

The oTemperaturen parameter is declared as output and of application-specific type "UDT_Temperaturen".

UDT_Temperaturen

	Name	Data type	Default value	Accessible from HMI/OPC UA/Web API	Writable from HMI/OPC UA/Web API	Visible in HMI engineering
1	Board	Struct		☑	☑	☑
2	Temp_1	Real	0.0	☑	☑	☑
3	Temp_2	Real	0.0	☑	☑	☑
4	Temp_3	Real	0.0	☑	☑	☑
5	Temp_4	Real	0.0	☑	☑	☑
6	Temp_5	Real	0.0	☑	☑	☑
7	Temp_6	Real	0.0	☑	☑	☑
8	Temp_7	Real	0.0	☑	☑	☑
9	Tip	Struct		☑	☑	☑
10	Temp_1	Real	0.0	☑	☑	☑
11	Temp_2	Real	0.0	☑	☑	☑
12	Temp_3	Real	0.0	☑	☑	☑
13	Temp_4	Real	0.0	☑	☑	☑
14	Temp_5	Real	0.0	☑	☑	☑
15	Temp_6	Real	0.0	☑	☑	☑
16	Temp_7	Real	0.0	☑	☑	☑

Fig. 32

The data type outputs the current temperatures of the sensors whereas a distinction is made between the board and tip temperature. If a sensor is deselected, both temperatures are marked with 555.5 °C. If a sensor is selected but it is offline (e.g. due to insufficient energy), the values 999.9 °C are output for both temperatures.

7.2.3.10 oStatus parameter

The oStatus parameter is declared as output and of application-specific type "UDT_Status".

UDT_Status

	Name	Data type	Default value	Accessible from HMI/OPC UA/Web API	Writable from HMI/OPC UA/Web API	Visible in HMI engineering
1	Receiver	Struct		☑	☑	☑
2	TRCV	Struct		☑	☑	☑
3	Error	Bool	false	☑	☑	☑
4	Status	Word	16#0	☑	☑	☑
5	TSEND	Struct		☑	☑	☑
6	Error	Bool	false	☑	☑	☑
7	Status	Word	16#0	☑	☑	☑
8	Verbindung_CPU	Struct		☑	☑	☑
9	Fehler	Bool	false	☑	☑	☑
10	Online	Bool	false	☑	☑	☑
11	Sensor_1	Struct		☑	☑	☑
12	MAC_Adresse	Struct		☑	☑	☑
13	Fehler	Bool	false	☑	☑	☑
14	Verbindung	Struct		☑	☑	☑
15	Online	Bool	false	☑	☑	☑
16	Temperatur	Struct		☑	☑	☑
17	Board	Struct		☑	☑	☑
18	Tip	Struct		☑	☑	☑
19	Sensor_2	Struct		☑	☑	☑
20	Sensor_3	Struct		☑	☑	☑
21	Sensor_4	Struct		☑	☑	☑
22	Sensor_5	Struct		☑	☑	☑
23	Sensor_6	Struct		☑	☑	☑
24	Sensor_7	Struct		☑	☑	☑

Fig. 33

The data type output various status information on the receiver and the activated sensors:

- Receiver:
  - Status to block TRCV_C
    - An error occurred in the communication
    - Status of communication (see the help in the ITA portal)
  - Status to block TSEND_C
    - An error occurred in the communication
    - Status of communication (see the help in the ITA portal)
  - Connection to CPU:
    - Connection error to the receiver (check cable, check receiver)
    - Online connection, i.e. connection between CPU and receiver in order
- Sensor x:
  - MAC address error (e.g. wrong length, wrong signs, ...)
  - Online connection, i.e. sensor sends data to receiver and/or CPU
  - Underflow or overflow - board and/or tip temperature
    - Underflow: Temperature less than or equal to -41 °C
    - Overflow: Temperature greater than or equal to 201 °C

7.2.4 Examples for visualization with WinCC

All sensors are activated.

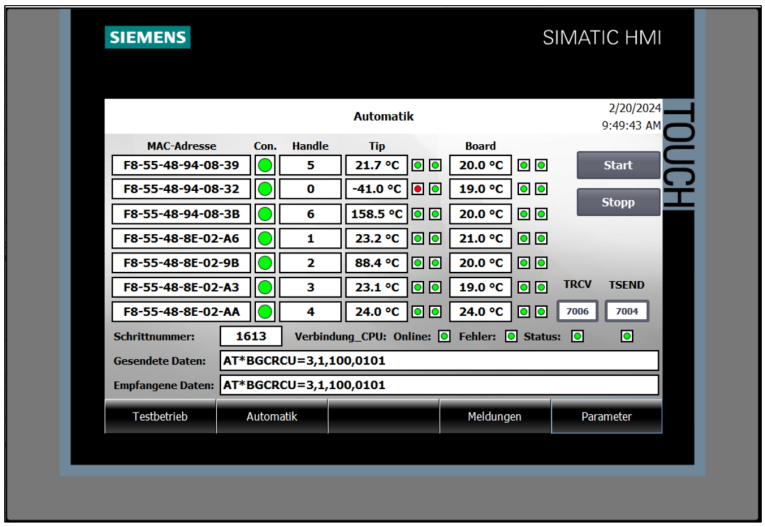


Fig. 34

Sensor No. 2 is deactivated (board and tip temperature display 555.5 °C).

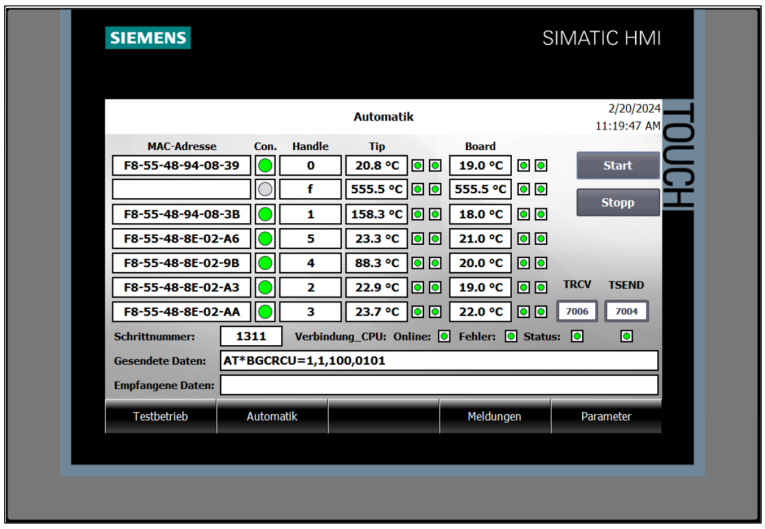


Fig. 35

Entry of MAC address.

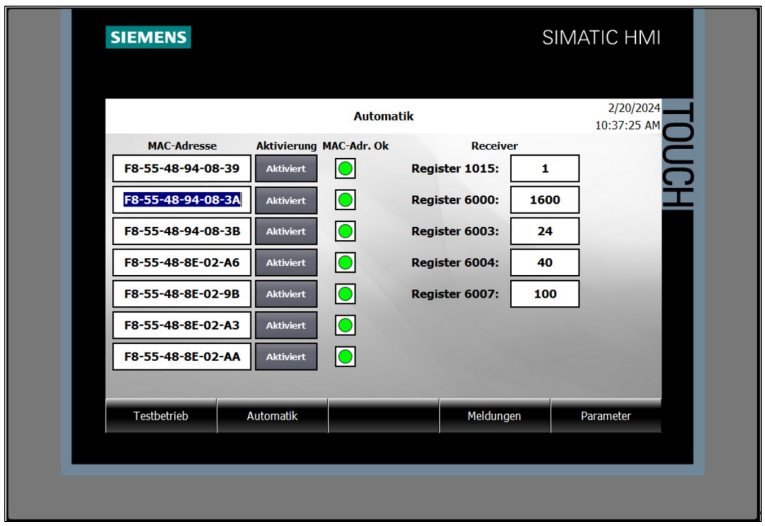
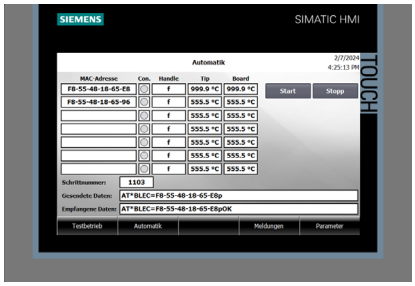
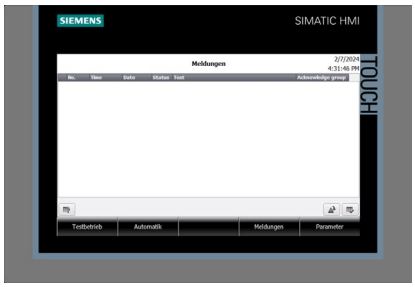


Fig. 36

7.2.5 Unit

7.2.5.1 Starting procedure

01		Switch on the main switch
02		Wait until CPU and visualization were started
02		Acknowledge pending malfunctions • Call up the messages operator display • Acknowledge the malfunctions • Eliminate the malfunction, if any

7.2.5.2 Start precondition

The following preconditions must be fulfilled so that automatic mode can take place:

- At least 1 sensor is activated
- No firewall between CPU and receiver
  100 meters per segment is the maximum length of the LAN cable
  The LAN cable must be shielded and correspond to at least Cat5 (100 Mbit/s).
- No error when entering the MAC addresses
- Automatic mode preselected
- No malfunction active

7.3 Allen-Bradley (Rockwell) CPU

Depending on the user's level of knowledge, there are two ways of integrating the required logic into the program.
On the one hand, the complete routines with all required tags and most of the configuration can be imported using "plug&play".
On the other hand, all tags and routines can be created manually and the two required AOIs imported.

Please note: It is not necessary to add hardware information to both procedures as the communication is realized by means of TCP stack.
However, an Ethernet communication device (e.g. EN2T or similarly preconfigured) is required.
Files contained:

- BLE_TempSens_Routine_RLL.L5X
- AOI_VBLE_TempSens_AOI.L5X
- AOI_TCP_CLIENT_AOI.L5X

7.3.1 Importing the complete routine

The installation package is contained in the complete routine under the name "BLE_TempSens_Routine_RLL.L5X".
This package can be imported directly into the existing program as shown in the following screenshots.

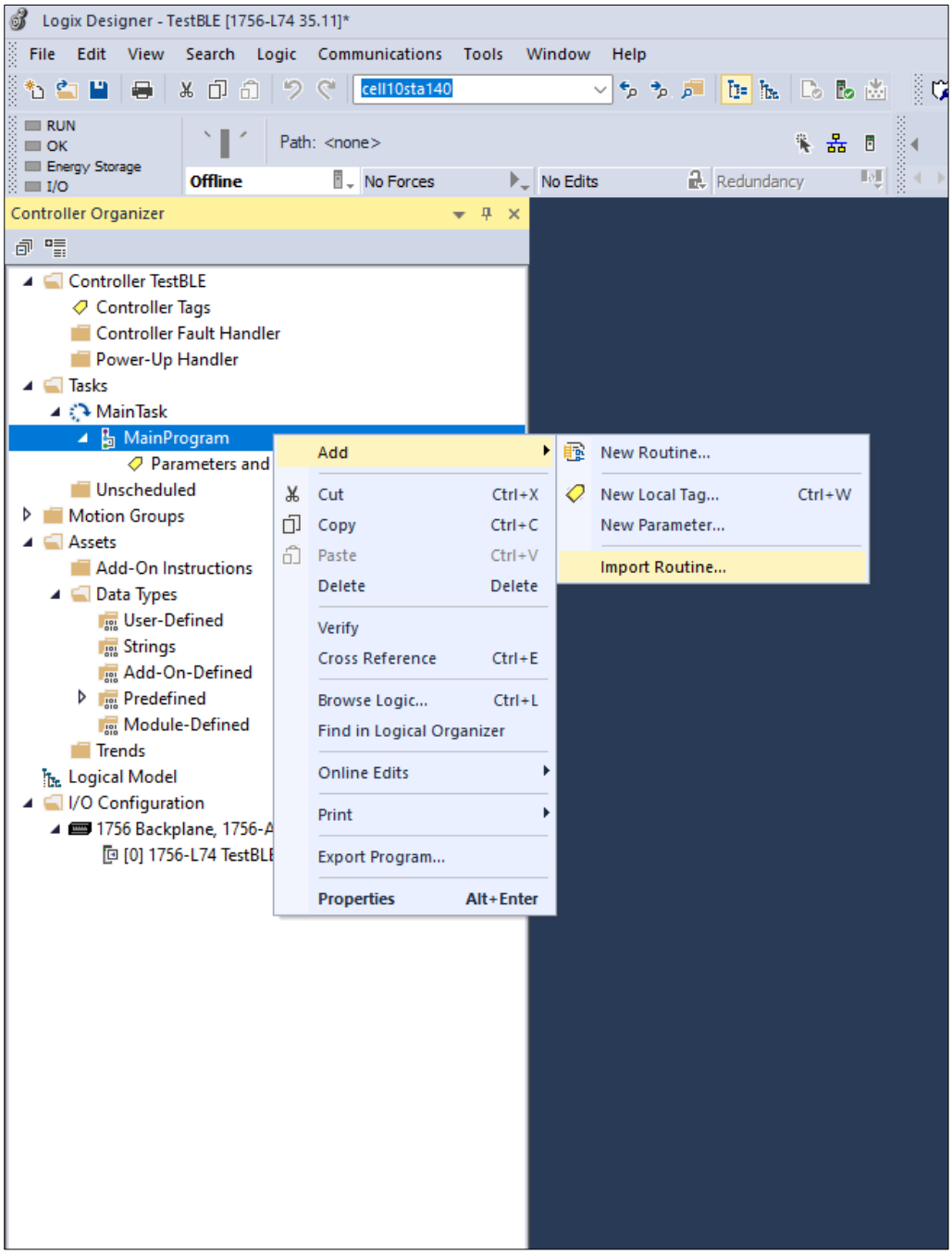

Logix Designer - TestBLE [1756-L74 35.11]*
File Edit View Search Logic Communications Tools Window Help
cell10sta140
RUN
OK
Energy Storage
I/O
Path: <none>
Offline
No Forces
No Edits
Redundancy
Controller Organizer
Controller TestBLE
Controller Tags
Controller Fault Handler
Power-Up Handler
Tasks
MainTask
MainProgram
Parameters and
Unscheduled
Motion Groups
Assets
Add-On Instructions
Data Types
User-Defined
Strings
Add-On-Defined
Predefined
Module-Defined
Trends
Logical Model
I/O Configuration
1756 Backplane, 1756-A
[0] 1756-L74 TestBLE
Add
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Delete Delete
Verify
Cross Reference Ctrl+E
Browse Logic... Ctrl+L
Find in Logical Organizer
Online Edits
Print
Export Program...
Properties Alt+Enter
New Routine...
New Local Tag... Ctrl+W
New Parameter...
Import Routine...

Fig. 37

After the import, the routing is displayed with the name "BLE_TempSens", in which only the Ethernet device used must be indicated.

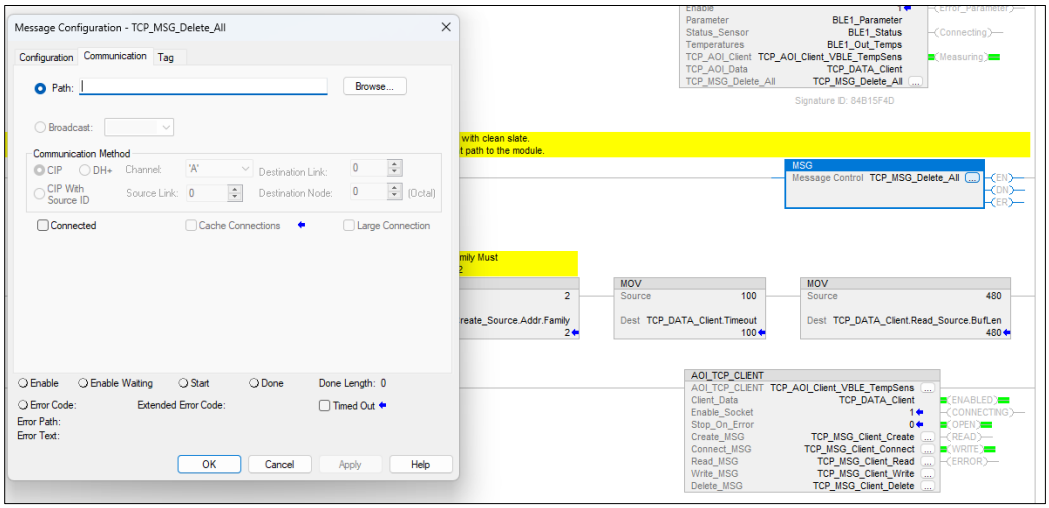


Fig. 38

Several message notes are indicated which can be edited by clicking on the three points next to the following tag names:

- TCP_MSG_Delete_All
- TCP_MSG_Client_Create
- TCP_MSG_Client_Connect
- TCP_MSG_Client_Read
- TCP_MSG_Client_Write
- TCP_MSG_Client_Delete

By opening the settings and navigating to the second tab, the path to the Ethernet device used must be set.

The installation is then completed and the device can be used.

7.3.2 Manual installation of routines

For experienced users, the two required AOIs are included and can be imported under "Assets → Add On Instructions" as follows:

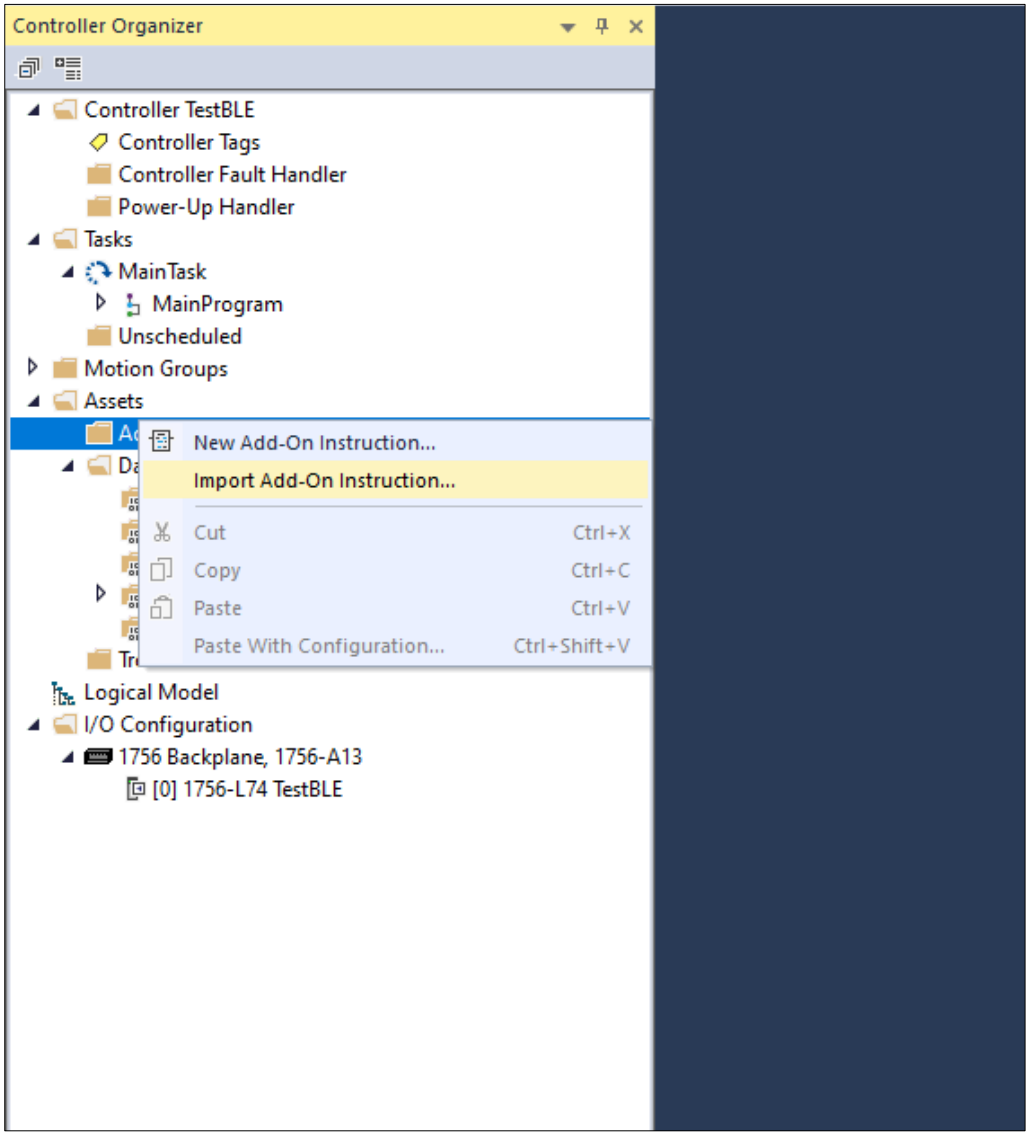


Fig. 39

This installs all the required commands and data types for the program. Please note that three options must be set in the TCP-Client-AOI for the correct communication type, as shown in the example routine:

After entering the commands in the program, the configuration of the message notes, which are contained in the TCP-Client, is required as follows:

7.3.2.1 Configuration of the “Delete_All” command

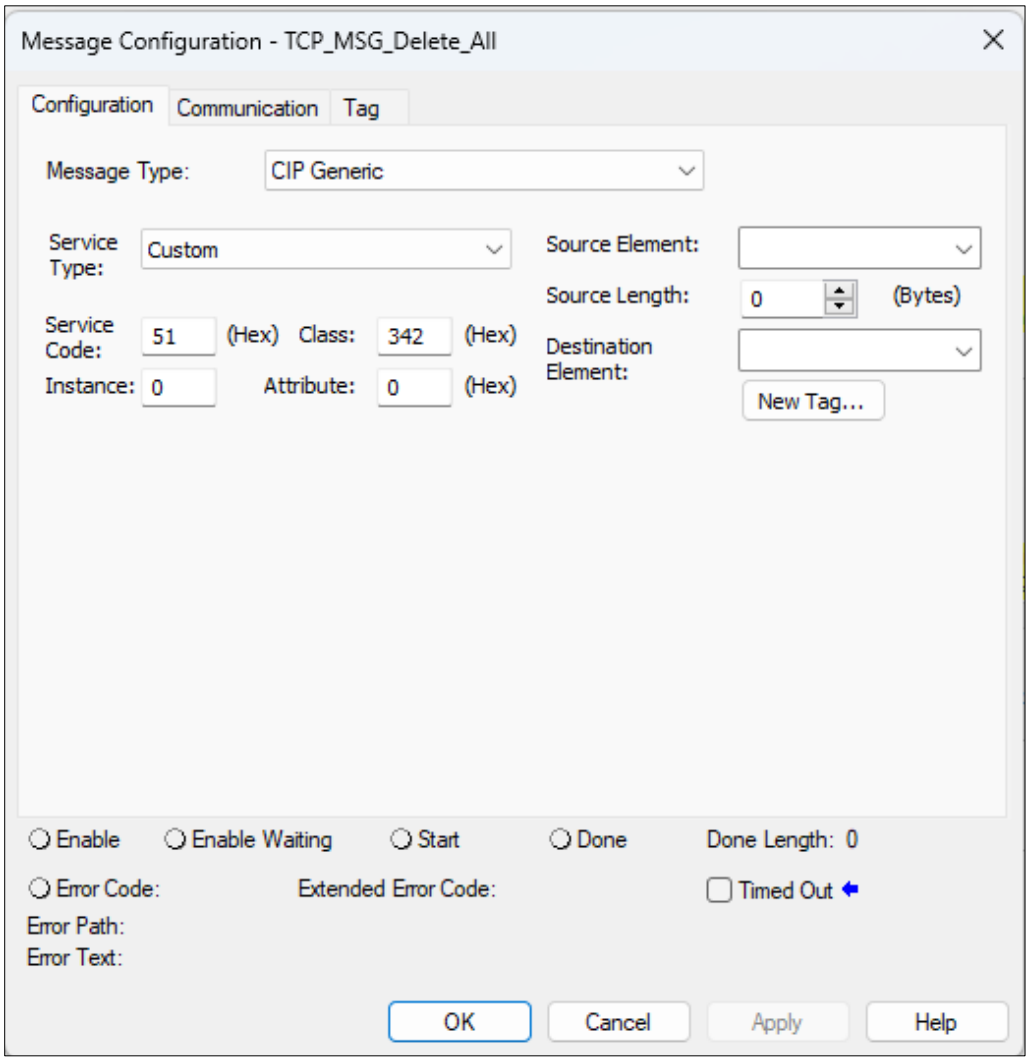


Fig. 40

7.3.2.2 Configuration of the “Create_MSG” command

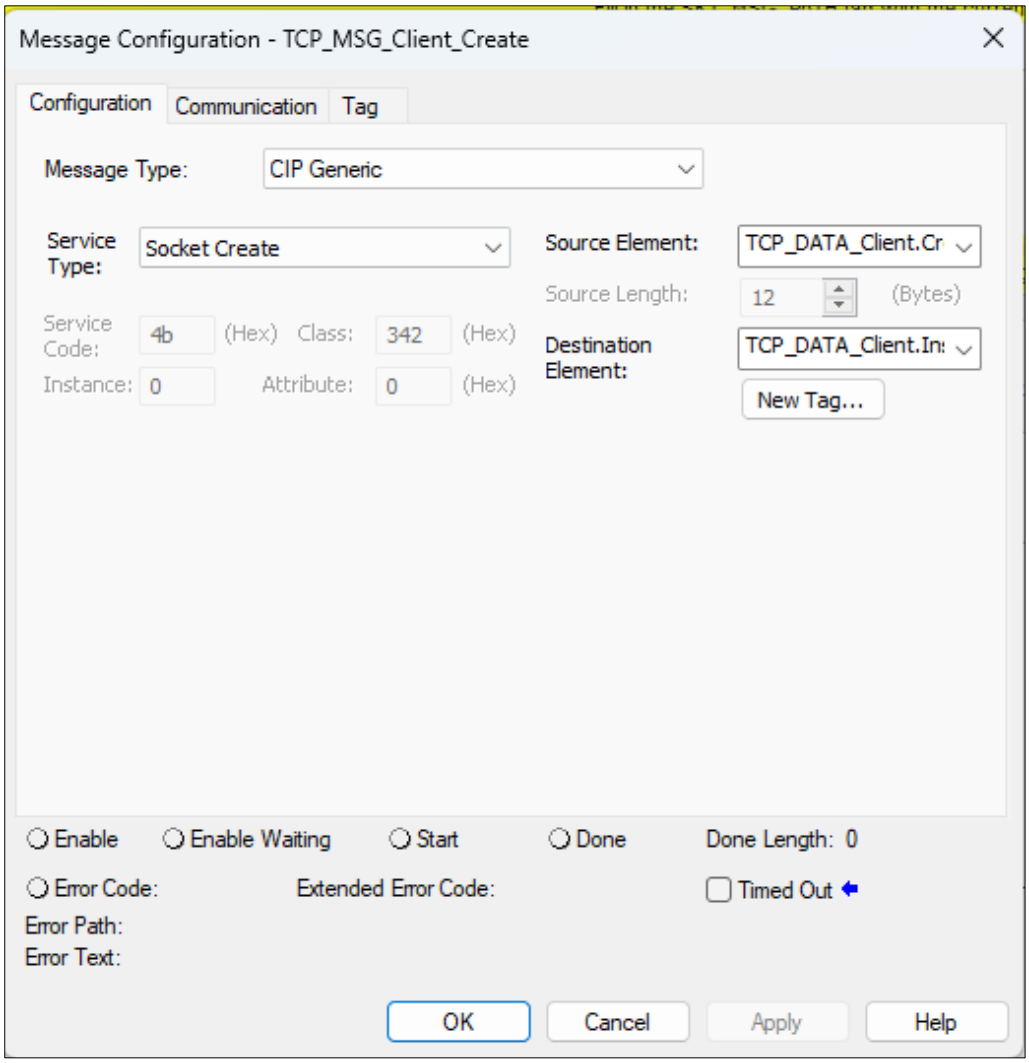


Fig. 41

7.3.2.3 Configuration of the “Connect_MSG” command

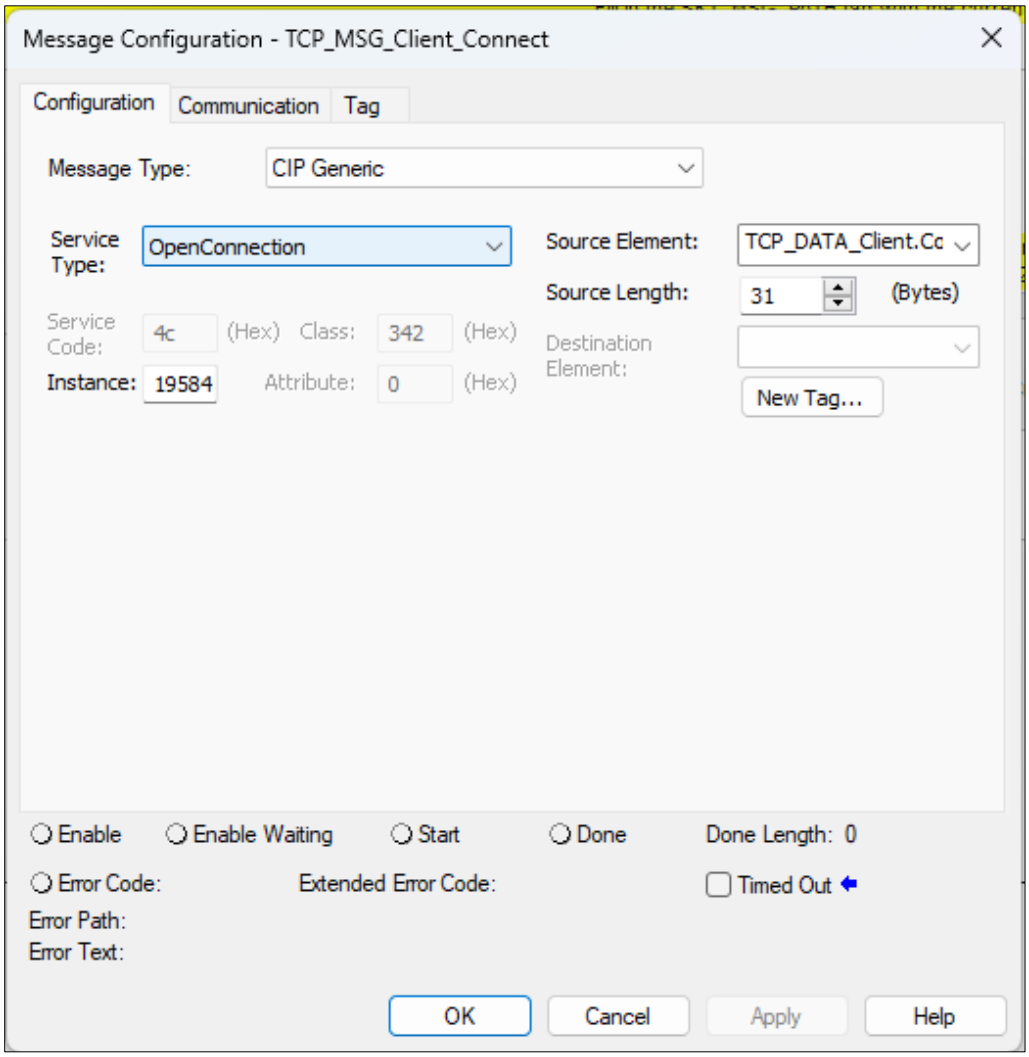


Fig. 42

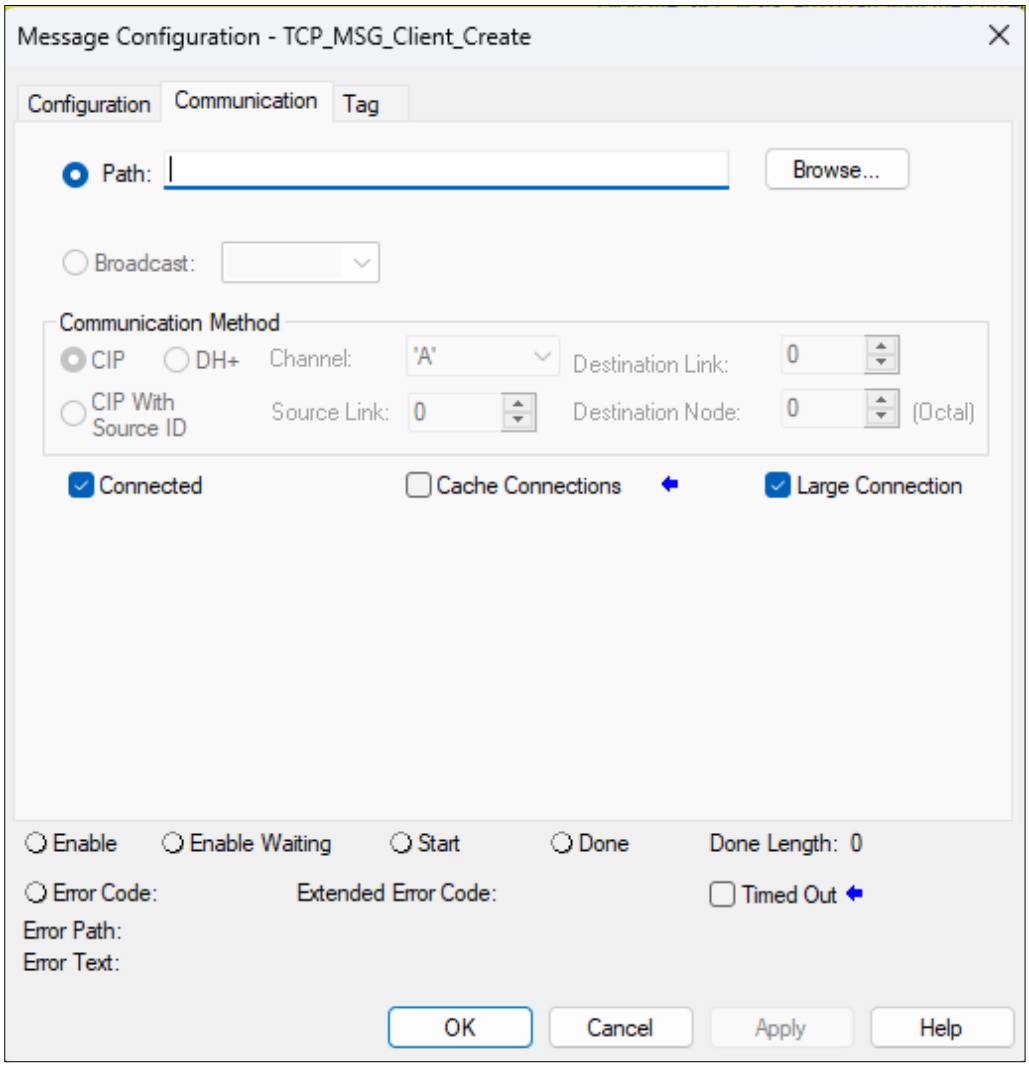

Message Configuration - TCP_MSG_Client_Create
Configuration
Communication
Tag
Path:
Browse...
Broadcast:
Communication Method
CIP
DH+
Channel:
'A'
Destination Link:
0
CIP With Source ID
Source Link:
0
Destination Node:
0
(Octal)
Connected
Cache Connections
Large Connection
Enable
Enable Waiting
Start
Done
Done Length: 0
Error Code:
Extended Error Code:
Timed Out
Error Path:
Error Text:
OK
Cancel
Apply
Help

Fig. 43

7.3.2.4 Configuration of the “Read_MSG” command

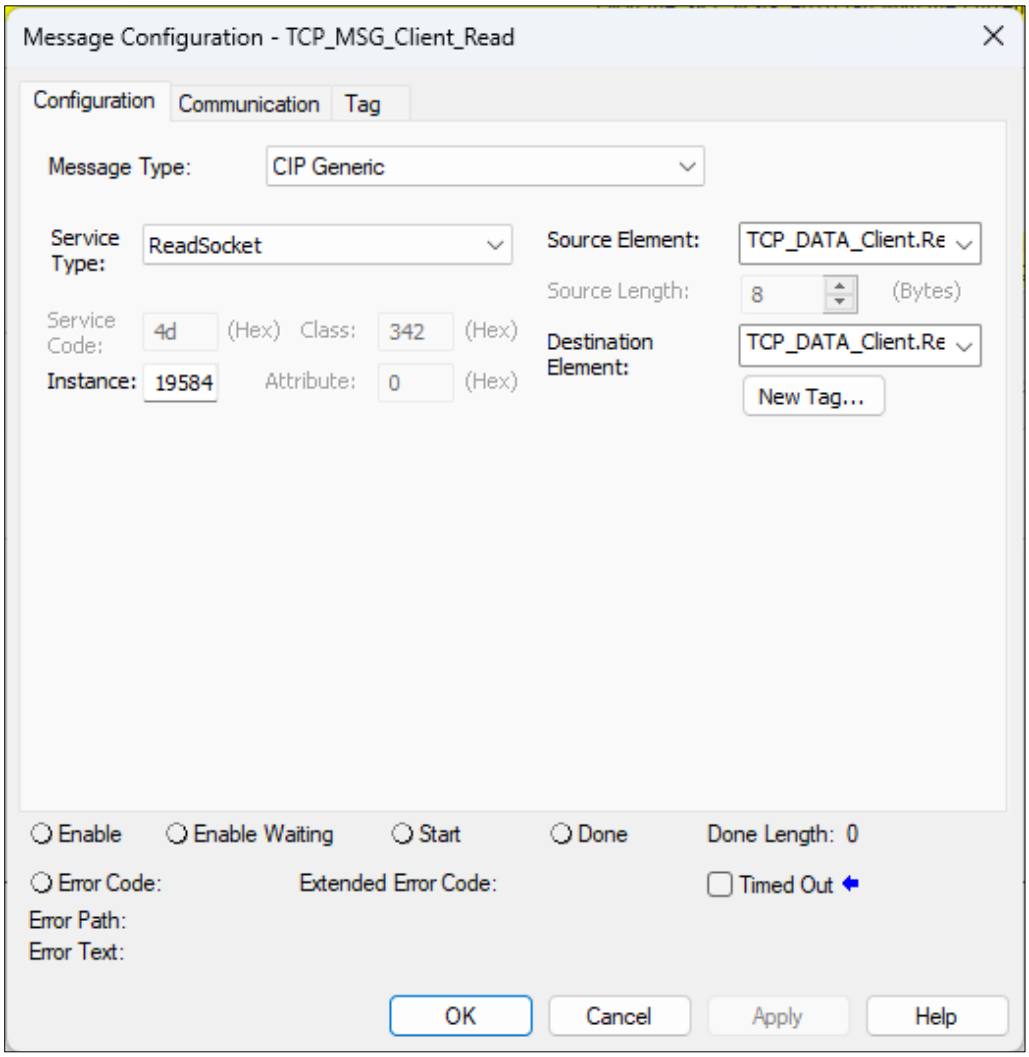


Fig. 44

7.3.2.5 Configuration of the “Write_MSG” command

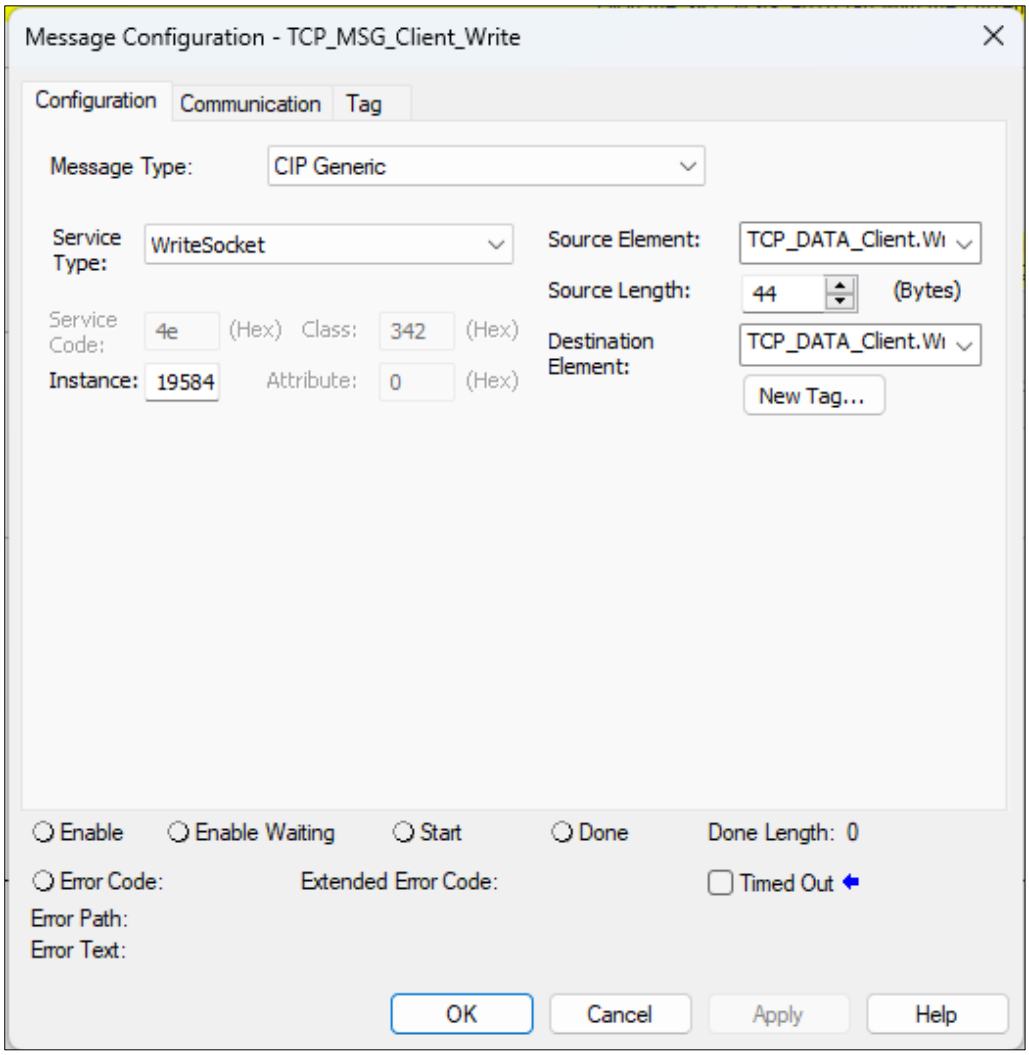


Fig. 45

7.3.2.6 Configuration of the “Delete_MSG” command

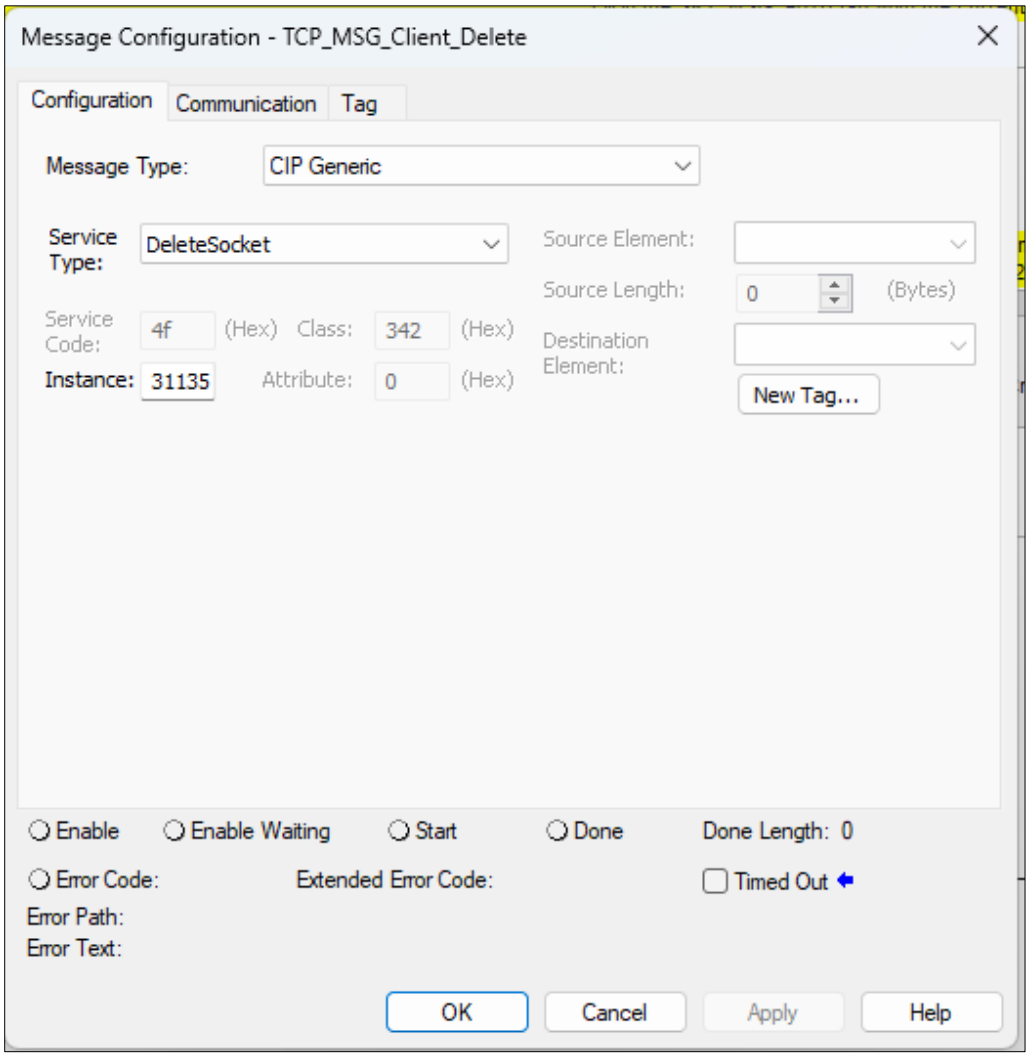


Fig. 46

7.3.3 Configuration of the temperature sensor and receiver

After completing the steps described in the complete or manual installation, the final configuration of the temperature sensors used can now be made.
For this, a tag called "BLE1_Parameter" with data type "udt_VBLE_TempSens_Parameters" was created in the local program, which is as follows:

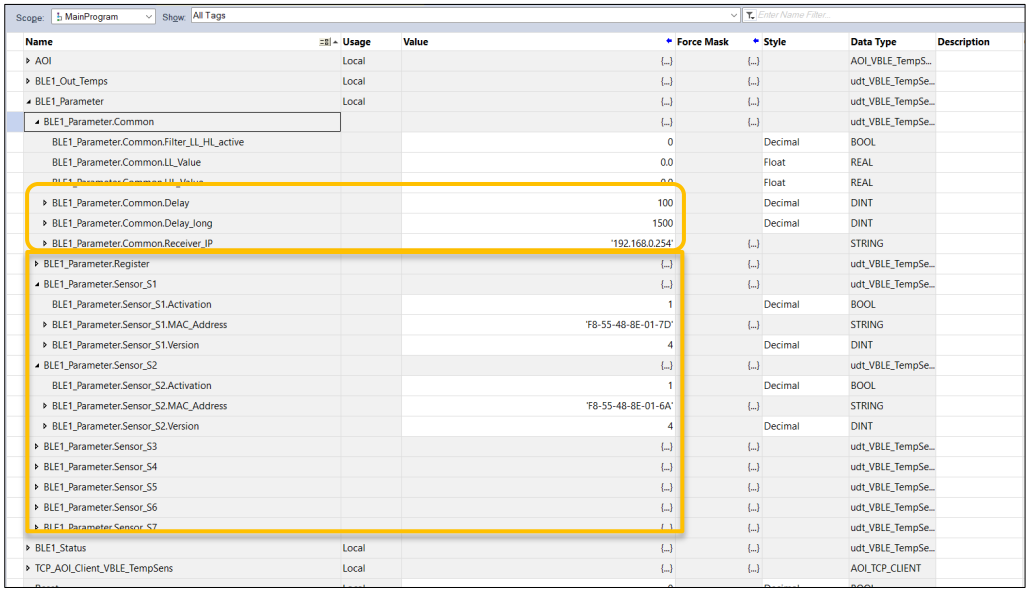


Fig. 47

Within these tags, the configuration of the used receiver interface and the temperature sensors can be entered.
The receiver interface only requires the IP used for the interface under "Common.Receiver_IP".

It is important to adapt the tags “Delay“ and "Delay_long" as shown on the following illustrations. This ensures the function.

For each temperature sensor (Sensor 1 to maximum Sensor 7), the MAC address, which is engraved on the respective sensor in the format XX-XX-XX-XX-XX-XX, and the sensor version must be entered.

7.3.4 Reception of temperature results from tags

After completion of the installation and starting of the temperature measurement by using the "Enable" tag from the command, communication with the receiver takes place. The current temperatures (tip and board temperature) are read out in real time, sorted by sensor and placed in tag "BLE1_Out_Temps" for further use.

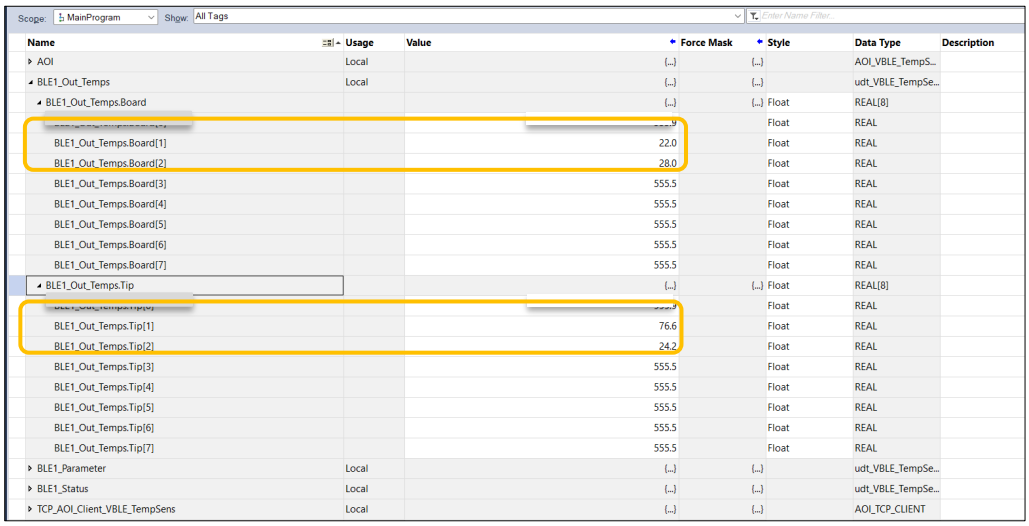


Fig. 48

7.3.5 Exemplary visualization using "FT View Studio"

Setting up the Sensor MAC addresses

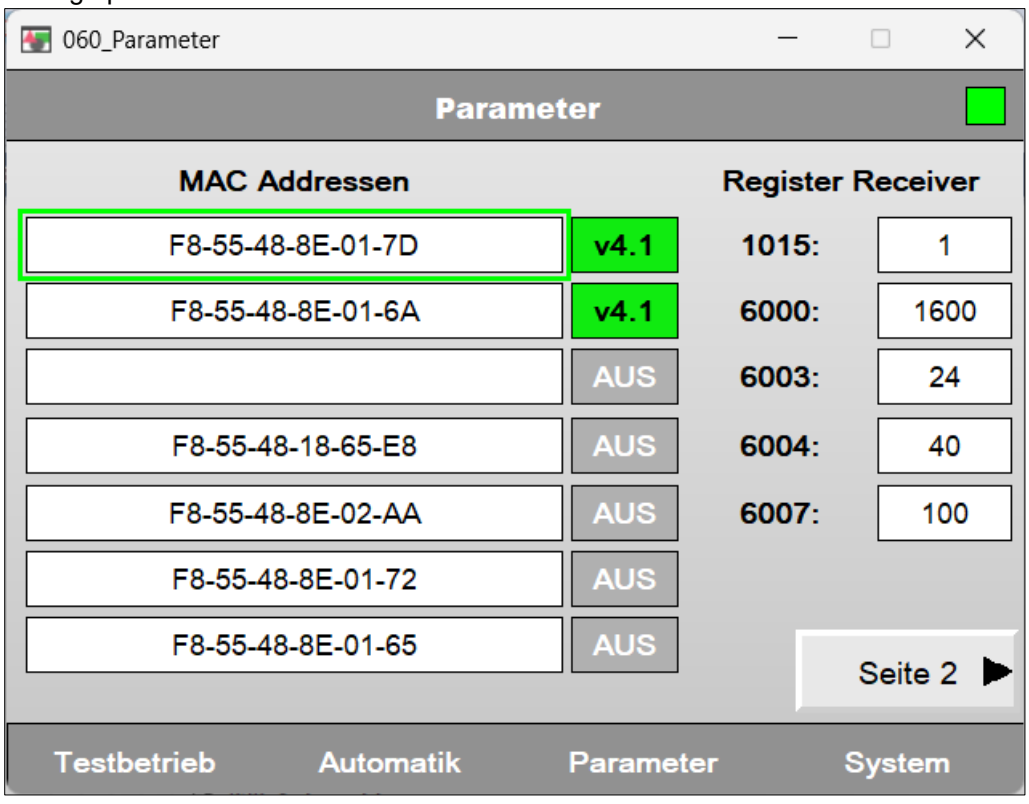


Fig. 49

Setting up the receiver IP address

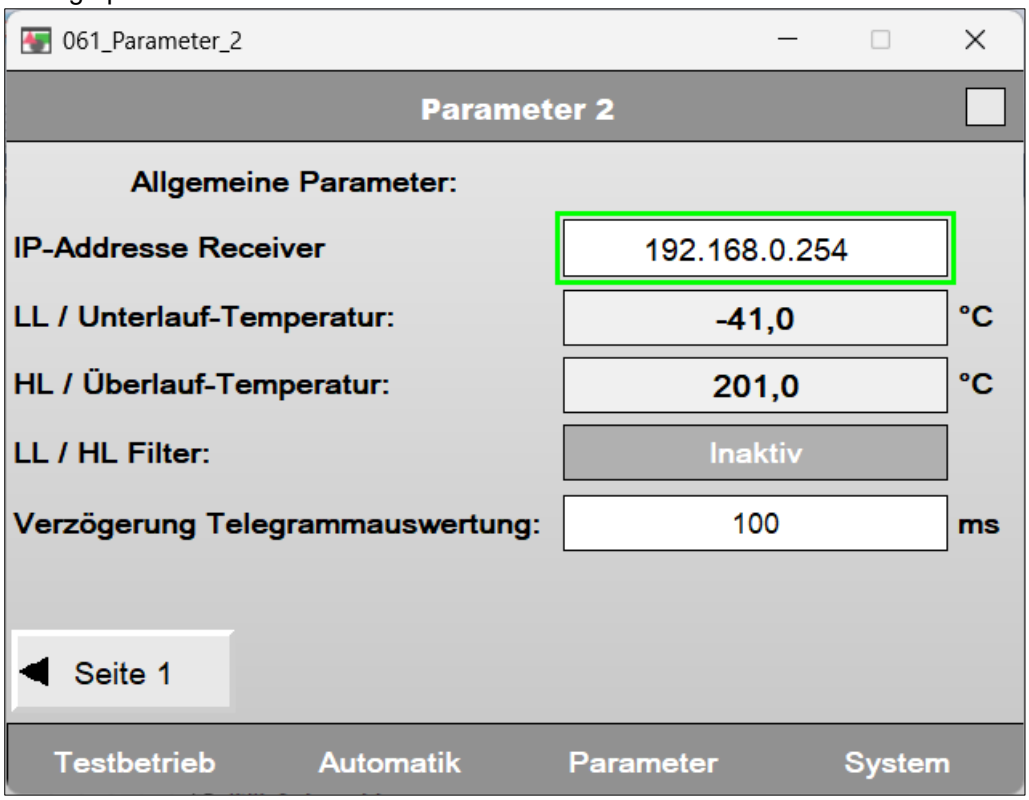


Fig. 50

Start of measurement

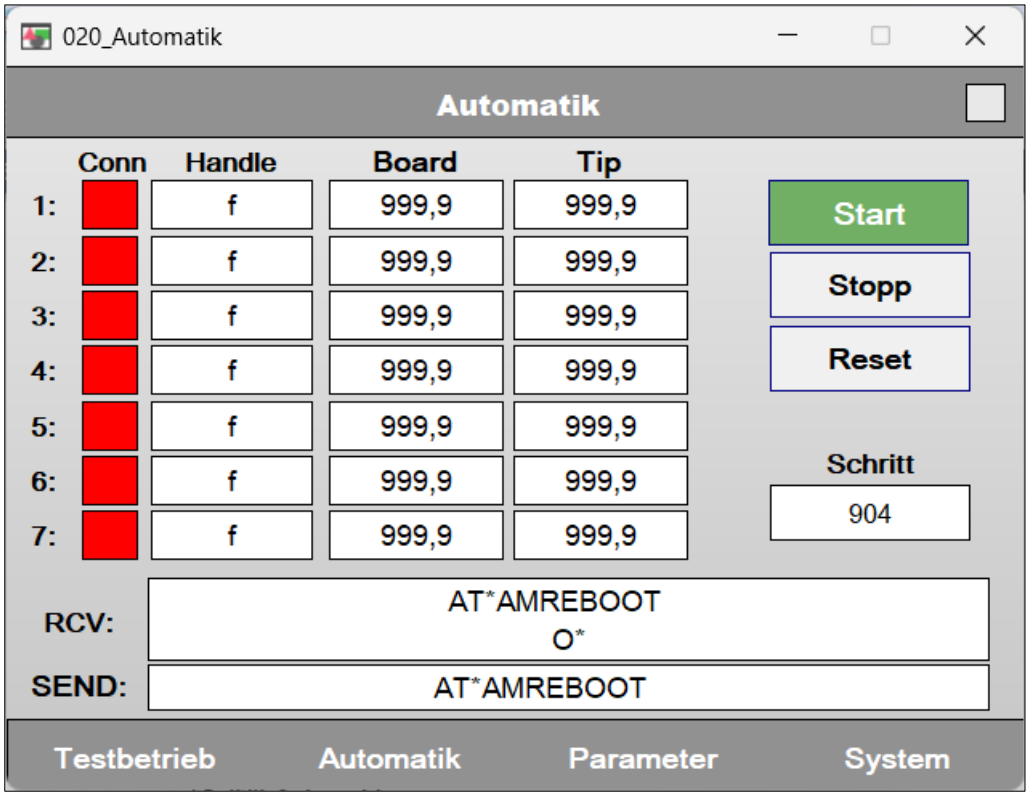


Fig. 51

The measurement is started and the temperature values are displayed

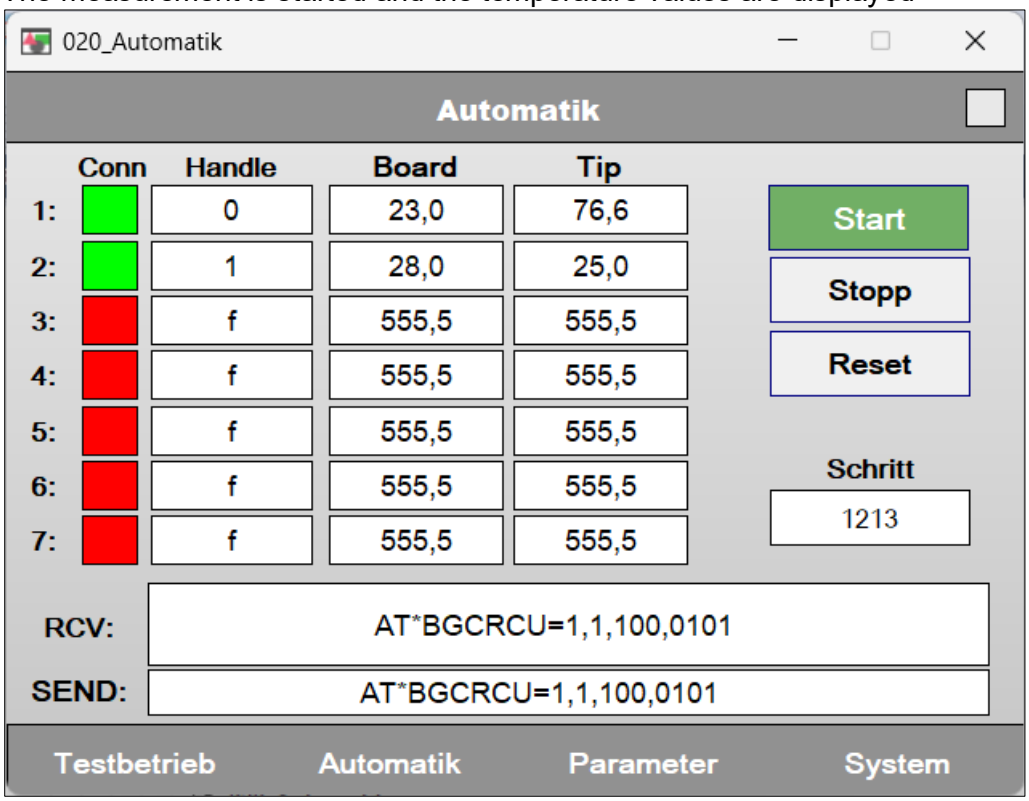


Fig. 52

7.3.6 Unit

7.3.6.1 Start precondition

The following preconditions must be fulfilled so that automatic mode can take place:

- At least 1 sensor is activated
- No firewall between CPU and receiver
- 100 meters per segment is the maximum length of the LAN cable
- The LAN cable must be shielded and correspond to at least Cat5 (100 Mbit/s)
- No error when entering the MAC addresses
- No malfunction active

8 Commissioning

⚠ WARNING

Risk of injury
Please observe, in particular, → Chapter 5 (Safety) when working on the non-contacting thermal measuring device (OnSens.SmarTemp)!

- A commissioning not performed properly could cause injury to persons, or harm to property and the environment!
- Experts only are allowed to perform commissioning, in particular, first starting of the turbo coupling!
- Secure the machine against unintentional switching on!
- After connection to the power supply, the receiver requires an initialization time of **about 10°s**, only then is the BTM-light ready for operation and the turbo coupling can be started.

- Check the wiring. Please pay special attention to the proper wiring of the supply voltage!
- Apply the supply voltage to the receiver.
- The receiver requires an initialization time of about 10 s.
- Normal operation can start now. In case of malfunctions, → Chapter 11.
- After starting the turbo couplings, the temperature sensor requires a certain amount of time to generate the required internal voltage. If the temperature of the operating medium is already more than approx. 20 Kelvin higher than the ambient temperature, this period is several seconds until the first temperature signal is sent. If the operating medium of the turbo coupling is heated to less than approx. 20 Kelvin in relation to the environment (e.g. longer standstill, no-load mode, operation with low load), the internal voltage supply is not sufficient and the temperature sensor does not send a stable continuous signal. The temperature sensor only starts stable signal transmission without interruptions after the required temperature difference of approx. 20 Kelvin was exceeded in a stationary state. In unsteady warmed-up state of the temperature sensor (e.g. machine start-up), the required temperature difference is up to 60 Kelvin. A corresponding bypass must be realized in the machine control system.

9 Maintenance, Servicing

Maintenance and Servicing: A combination of all activities conducted in order to maintain an object in a condition or to re-store it to such a condition which meets the requirements of the respective specification and ensures performance of the required functions.

Inspection: An activity involving the thorough examination of an object in order to provide a reliable statement as to the condition of said object, performed without disassembly or, if necessary, with only partial disassembly, supplemented by measures such as the taking of measurements.

Visual inspection: A visual inspection is an inspection in which visible defects, such as missing screws or bolts, are identified without the use of access equipment or tools.

Close-up inspection: An inspection in which, in addition to the areas covered by the visual inspection, defects such as loose bolts, that can only be detected by using access equipment, e.g. mobile stair steps (if required) and tools are identified. For close-up inspections, usually a housing does not need to be opened or the power to the equipment be cut off.

Detailed inspection: An inspection in which, in addition to the areas covered by the close-up inspection, defects such as loose connections, that can only be detected by opening housings and/or using tools and test equipment (if required) are identified.

⚠ WARNING

Risk of injury
Please observe, in particular, → Chapter 5 (Safety) when working on the non-contacting thermal measuring device (OnSens.SmarTemp)!
- Please always keep access paths free to the turbo coupling!

Qualification
→ Chapter 5.8

- Skilled and authorized persons only are allowed to carry out maintenance and repair work! Qualification is ensured by performing training and giving instructions on the turbo coupling.
- Possible consequences of improper servicing and maintenance could be death, serious or minor injuries, damage to property and harm to the environment.

- Switch off the unit in which the turbo coupling is installed and secure the switch against inadvertent switch-on.
- For all work performed on the turbo coupling ensure that both the drive motor and the driven machine have stopped running and that unintended starting is absolutely impossible!
- Components may only be replaced by original spare parts.

Re-mount all protective covers and safety devices in their original position immediately after completion of the servicing and maintenance work. Check them for proper functioning.

Maintenance schedule:

Time	Maintenance work
3 months after commissioning at the latest, then every year	Inspect the machine for irregularities (visual inspection).
	Check the electrical system for sound condition (detailed inspection).
In case of impurities	Cleaning (→ Chapter 9.1).

Table 7

- Carry out any maintenance work and routine inspections according to the report.
- Record the maintenance work carried out.

Report templates → Operating manual of turbo coupling

9.1 Outside cleaning

NOTICE

Damage to property
Damage to the OnSens.SmarTemp due to an improper, unsuitable outside cleaning.
- Ensure that the cleaning agent is compatible with the grouting compound of the OnSens.SmarTemp!
- Do not use high-pressure cleaning equipment!
- Be careful with seals. Do not apply a water and compressed-air jet.

- Clean the OnSens.SmarTemp with a degreasing agent, as and when required.

10 Disposal

Disposal of the packaging
Dispose of packaging material according to the local regulations.

How to dispose of operating fluids
On disposal, please observe the applicable laws and the producer's or supplier's instructions.

Disposal of the OnSens.SmarTemp
Dispose of the OnSens.SmarTemp according to the local regulations.

For special information on the disposal of the substances and materials used, please see the following table:

	Kind of disposal		
Material / substance	**Reuse**	**Residual waste**	**Special waste**
Metals	x	-	-
Cables	x	-	-
Seals	-	x	-
Plastics	x [1)]	(x)	-
Operating media	-	-	x [1), 2)]
Packing	x	-	-

Table 8

1) If possible
2) Disposal according to the safety data sheet or the manufacturer's instructions

11 Malfunctions - Remedial Actions, Troubleshooting

⚠ WARNING

Risk of injury
Please observe, in particular, → Chapter 5 (Safety) when working on the non-contacting thermal measuring device (OnSens.SmarTemp)!

The following table is intended to help finding the cause of malfunctions or problems quickly and to take remedial action, if necessary.

Malfunction	Possible cause(s)	Remedial action	See
The receiver has no display ("PWR" LED does not light up).	Power supply is missing, incorrect or poles are reversed.	Check the power supply and wiring. Properly apply/switch on the power supply.	Chapter 6.4
	The receiver is defective.	Replace the receiver.	

Malfunction	Possible cause(s)	Remedial action	See
Machine control system does not receive a temperature signal (or temperature signal 999.9 °C)	Data cable between receiver and machine control system is not properly connected ("LAN" LED does not light up)	Check the data cable wiring to the superimposed control system.	
	receiver is not properly integrated in the machine control system.	Check the implementation.	Chapter 7
	Incorrect sensor MAC address is stored in the machine control system.	Compare the MAC address (engraved on the sensor) with the entry and correct.	Chapter 7.2
	Temperature of the operating medium of the turbo coupling is less than 20 Kelvin above ambient temperature	Increase the operating medium temperature, e.g. by increasing the load capacity of the driven machine.	Chapter 2.1
	Signal range, distance between temperature sensor and receiver too great	Mount the receiver within the range of the temperature sensor. Avoid shielding (e.g. closed cabinet).	Chapter 6.4
	Temperature sensor is defective.	Check the temperature sensor for damage, replace the temperature sensor, if required.	
Machine control system only sporadically receives no temperature signal (or temperature signal 999.9 °C)	Temperature of the operating medium of the turbo coupling is slightly lower or close to 20 Kelvin above ambient temperature	Increase the operating medium temperature, e.g. by increasing the load capacity of the driven machine.	Chapter 2.1
Temperature output is incorrect.	Receiver is not properly integrated in the machine control system.	Check the implementation.	Chapter 7
	Temperature sensor is defective.	Check the temperature sensor for damage, replace the temperature sensor, if required.	

Malfunction	Possible cause(s)	Remedial action	See
Leaks on the turbo coupling	Leak on the temperature sensor fitting or OnSens.SmarTemp blind screw	Check the sealing ring for proper seat, check the tightening torque	Chapters 6.2 and 6.3
Loss of operating medium through the fusible plugs.	Equipment monitoring is not correctly matched to the response temperature or fusible plugs (FP), temperature drift of OnSens.SmarTemp is not regarded properly.	Check the temperature monitoring of the equipment control system. Properly regard the temperature drift of the OnSens.SmarTemp. Contact Voith, if necessary.	Chapter 3.1
	Temperature of Voith turbo coupling (VTC) is too high on motor start-up.	Observe the cooling down time, if necessary measure the temperature manually before starting the motor.	
	Overload; which has not been regarded when designing the VTC.	Ensure the proper operation, avoid impermissible overload.	
	Load reduction in case of excess temperature too low or too late.	Determine the reaction of the system in case of load changes. Optimize the load reduction (operator/software).	
	Switch-off too late in case of excess temperature.	Determine the reaction of the system to a switch-off. Optimize the switch-off (operator/software).	
	The temperature output is too low.	See malfunction "Temperature output is incorrect".	
Please consult Voith (→ Chapter 12), if a malfunction occurs which is not included in this table.			

Table 9

12 Queries, Orders Placed for Field Service Engineers and Spare Parts

For

- queries
- Ordering a field service engineer
- Ordering spare parts
- commissionings

we need:

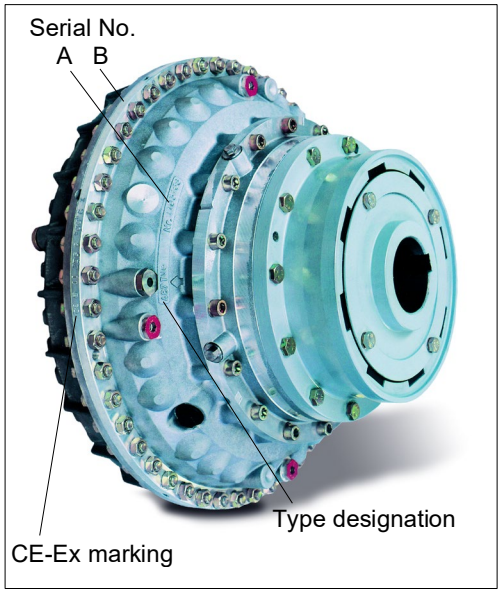


Fig. 53

the **Serial No.** and **type designation** of the turbo coupling on which the OnSens.SmarTemp is used.

→ You will find the serial number and type designation either on the outer wheel / coupling shell (A) or on the turbo coupling periphery (B).

→ The serial number is stamped in with figure stamps.

→ For turbo couplings, intended for the use in potentially explosive atmospheres, you will find the CE-Ex marking on the turbo coupling periphery.

When placing an order for a **field service representative**, **commissioning** or a **service**, we need, in addition

- the turbo coupling installation site,
- the name and address of a contact person,
- details of the malfunction/problem occurred.

Contact,
→ Page 2

When placing a **spare parts order**, we need, in addition,

- the shipping address for the spare parts shipment.

13 Spare Parts Information

NOTICE

Unauthorized changes or retrofits are not allowed to be performed on the coupling!
Do not retrofit accessories or equipment originating from other manufacturers!
Any changes or conversions performed without the prior written consent of Voith Turbo will result in the loss of any warranty! Any claims will forfeit!

- Professional maintenance or repair can only be guaranteed by the manufacturer!

13.1 Temperature sensor

Temperature sensor			Sealing ring
Use for turbo coupling size	**Dimension of thread**	**Material No.**	**Material No.**
366 - 650	M18x1.5	201.04653810	TCR.03658018
750 - 1330	M24x1.5	201.04653910	H01.105249

Table 10

13.2 OnSens.SmarTemp blind screws

Blind screw			Sealing ring
Use for turbo coupling size	**Dimension of thread**	**Material No.**	**Material No.**
366 - 650	M18x1.5	201.04461010	TCR.03658018
750 - 1330	M24x1.5	201.04461110	H01.105249

Table 11

13.3 Stationary receiver

Use for turbo coupling size	**Material No.**
366 – 1330	201.04641410

Table 12

13.3.1 Power supply cable 5 meters

Use for turbo coupling size	**Material No.**
366 – 1330	201.04460210

Table 13

13.3.2 Network cable 5 meters

Use for turbo coupling size	**Material No.**
366 – 1330	201.04460310

Table 14

14 Annex

EU Declaration of Conformity

Manufacturer:	J.M. Voith SE & Co. KG Voithstraße 1 74564 Crailsheim, GERMANY
Designation:	**Non-contacting thermal measuring device**
Type:	**OnSens.SmarTemp**

The non-contacting thermal measuring device consists of the following:

- OnSens.SmarTemp-Sensor (temperature sensor)
- OnSens.SmarTemp blind screw
- Stationary receiver

The manufacturer is solely responsible for the issuance of this declaration of conformity.

The above-described non-contacting thermal measuring device satisfies the following relevant harmonization legislation of the Union:

- 2014/53/EU (Radio Equipment Directive) / 22.5.2014 | EN | Official Journal of the European Union | L 153/62
- 2011/65/EU (RoHS Directive) / 08.6.2011 | EN | Official Journal of the European Union | L 174/88

The following harmonized standards (or parts thereof) have been applied:

- EN 300 328 V2.2.2

Other applied standards and technical specifications:

- EN IEC 62368-1:2020+A11:2020
- EN 301 489-1 V2.2.3:2019-11

Signed for and on behalf of J.M. Voith SE & Co. KG:

Berroth, Hannes

Digital unterschrieben von Berroth, Hannes
Datum: 2026.05.12 09:16:51 +02'00'

Crailsheim	11.05.2026	Hannes Berroth (Vice President CCE HDC)
Place	**Date:**	**Name, position, signature**

ENGLISH

Anybus® Wireless Bridge II Ethernet™

USER MANUAL

SCM-1202-032
Version 2.40
Publication date 2025-07-10

Important User Information

Disclaimer

The information in this document is for informational purposes only. Please inform HMS Networks of any inaccuracies or omissions found in this document. HMS Networks disclaims any responsibility or liability for any errors that may appear in this document.

HMS Networks reserves the right to modify its products in line with its policy of continuous product development. The information in this document shall therefore not be construed as a commitment on the part of HMS Networks and is subject to change without notice. HMS Networks makes no commitment to update or keep current the information in this document.

The data, examples and illustrations found in this document are included for illustrative purposes and are only intended to help improve understanding of the functionality and handling of the product. In view of the wide range of possible applications of the product, and because of the many variables and requirements associated with any particular implementation, HMS Networks cannot assume responsibility or liability for actual use based on the data, examples or illustrations included in this document nor for any damages incurred during installation of the product. Those responsible for the use of the product must acquire sufficient knowledge in order to ensure that the product is used correctly in their specific application and that the application meets all performance and safety requirements including any applicable laws, regulations, codes and standards. Further, HMS Networks will under no circumstances assume liability or responsibility for any problems that may arise as a result from the use of undocumented features or functional side effects found outside the documented scope of the product. The effects caused by any direct or indirect use of such aspects of the product are undefined and may include e.g. compatibility issues and stability issues.

Contact Information

Postal address:
Box 4126
300 04 Halmstad, Sweden

E-Mail: info@hms.se

Table of Contents

1. Preface

1.1. About This Document

This document describes how to install and configure Anybus® Wireless Bridge II Ethernet™.

For additional documentation and software downloads, FAQs, troubleshooting guides and technical support, please visit www.hms-networks.com/technical-support.

1.2. Document Conventions

Lists

Numbered lists indicate tasks that should be carried out in sequence:

1. First do this
2. Then do this

Bulleted lists are used for:

- Tasks that can be carried out in any order
- Itemized information

User Interaction Elements

User interaction elements (buttons etc.) are indicated with bold text.

Program Code and Scripts

```
Program code and script examples
```

Cross-References and Links

Cross-reference within this document: Document Conventions (page 1)

External link (URL): www.hms-networks.com

Safety Symbols

DANGER
Instructions that must be followed to avoid an imminently hazardous situation which, if not avoided, will result in death or serious injury.

WARNING
Instructions that must be followed to avoid a potential hazardous situation that, if not avoided, could result in death or serious injury.

CAUTION
Instruction that must be followed to avoid a potential hazardous situation that, if not avoided, could result in minor or moderate injury.

IMPORTANT
Instruction that must be followed to avoid a risk of reduced functionality and/or damage to the equipment, or to avoid a network security risk.

Information Symbols

NOTE
Additional information which may facilitate installation and/or operation.

TIP
Helpful advice and suggestions.

1.3. Trademarks

Anybus® is a registered trademark and Wireless Bridge II Ethernet™ is a trademark of HMS Networks AB.

All other trademarks are the property of their respective holders.

2. Safety

2.1. General Safety

CAUTION
This equipment emits RF energy in the ISM (Industrial, Scientific, Medical) band. Make sure that all medical devices used in proximity to this equipment meet appropriate susceptibility specifications for this type of RF energy.

CAUTION
This equipment contains parts that can be damaged by electrostatic discharge (ESD). Use ESD prevention measures to avoid damage.

CAUTION
This equipment is recommended for use in both industrial and domestic environments. For industrial environments it is mandatory to use the functional earth connection to comply with immunity requirements. For domestic environments the functional earth must be used if a shielded Ethernet cable is used, in order to meet emission requirements.

2.2. External Antenna Restrictions

For models with external antenna, only use antennas that are certified for use with this equipment.

Using external antennas that are not certified for use with this equipment will invalidate its certifications and make it non-compliant with the regulations for radio equipment.

A list of certified antennas can be found at www.hms-networks.com/technical-support.

2.3. Intended Use

The intended use of this equipment is as a communication interface and gateway. The equipment receives and transmits data on various physical levels and connection types.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

3. Cybersecurity

3.1. General Cybersecurity

IMPORTANT
To physically secure equipment and to prevent unauthorized access, it is recommended to install the equipment in a environment with access control.

IMPORTANT
To maintain the cybersecurity of the Bridge II Ethernet, only connect its Local Area Network (LAN) port to a trusted network.

Networks that are outside your security measures, such as firewalls and network administration, are considered untrusted. These networks are more vulnerable to unauthorized access and other security threats.

Examples of trusted networks include:

- Internal Company Local Area Networks (LANs): Managed and secured by the IT department.
- Industrial Control System (ICS) Networks: Used to control and monitor industrial processes, and can be isolated from other networks.
- Direct Connections: For example, a laptop connected with a LAN cable directly to the Bridge II Ethernet.

IMPORTANT
The Bridge II Ethernet can be manipulated through the digital input without authentication.

To maintain the cybersecurity of the Bridge II Ethernet, only connect its digital input to trusted devices.

Unauthenticated or unmonitored devices are considered untrusted and more vulnerable to unauthorized access and other security threats.

For a device to be considered trusted, it must come from reputable sources that follow security policies.

Trusted devices are verified and regularly monitored to ensure they do not pose a security risk.

IMPORTANT
To reduce the risk of sensitive data exposure, always perform a factory reset before decommissioning the equipment.

A factory reset will reset any on-site made configuration changes and revert the Bridge II Ethernet to the default settings of the latest installed firmware version.

See Reset to Factory Default (page 75).

3.2. Security Advisories

For cybersecurity reasons, stay informed about new vulnerabilities and follow the recommended actions.

HMS Networks Security Advisories includes information about our product vulnerabilities and available solutions.

You find our Safety Advisories at www.hms-networks.com/cybersecurity/security-advisories.

3.3. How to Report a Vulnerability

HMS Networks place the utmost importance on the security of our products and systems, however, despite all the measures we take, it cannot be excluded that vulnerabilities persist.

To report a potential vulnerability in an HMS product or service, please visit www.hms-networks.com/cybersecurity/report-a-vulnerability and follow the instructions.

3.4. Product Cybersecurity Context

3.4.1. Bridge II Ethernet Interfaces

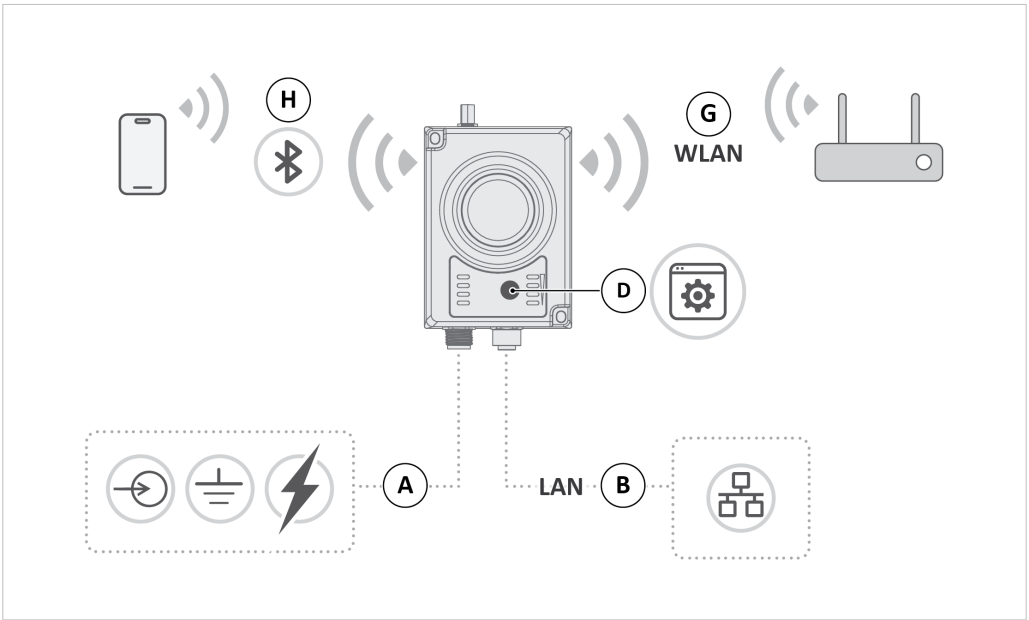


Figure 1. Bridge II Ethernet interfaces

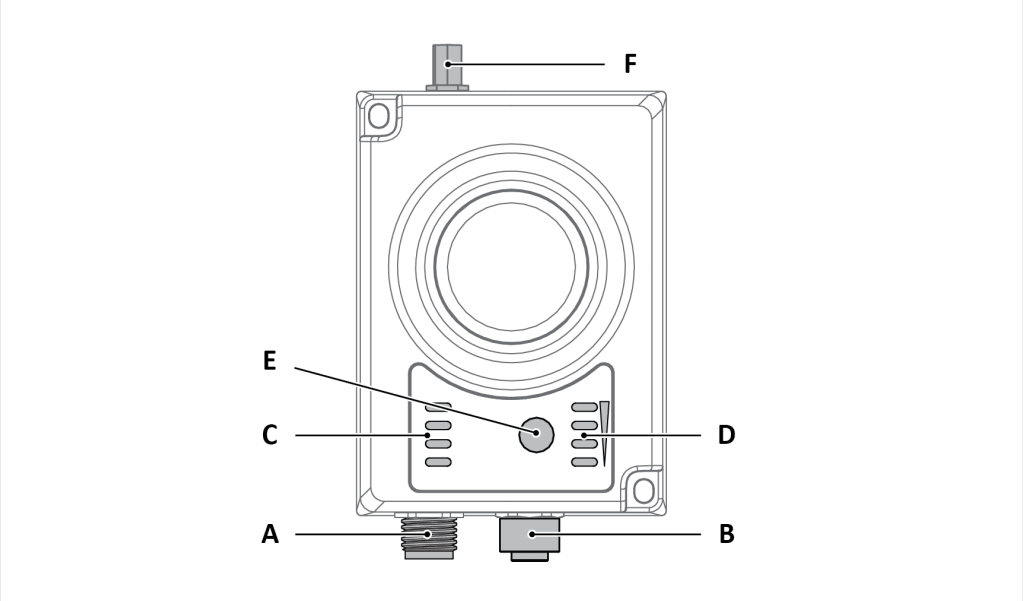


Figure 2. Bridge II Ethernet External parts

A. Power and Digital input interfaces
B. LAN interface
C. Status LED Indicators
D. Link Status LED Indicators
E. Mode button, configuration interface
F. For models with external antenna: Antenna connector
G. WLAN interface
H. Bluetooth interface

3.4.2. Services

Service	Description	Default Interface	Default Setting	Configurable Service
HTTP (Hypertext Transfer Protocol)	Enables configuration of the equipment over a network.	LAN	Restricted to local network only.	Restricted to local network only/ unrestricted.
DHCP (Dynamic Host Configuration Protocol) Server	Used to automatically assigns IP addresses and other network settings to devices on a network.	Applicable to all interfaces.	Off	Yes
Ping	Used by network devices to identify and locate other devices on a network.	Applicable to all interfaces.	On	No
Ethernet Tunnel	Used for tunneling of Ethernet Protocol Data Units (PDUs) between Anybus Wireless Bolt or Anybus Wireless Bridge II devices. Uses EtherType 0x6789.	Applicable to all interfaces.	Off	Yes
AT Command Interface on TCP/IP	Used for configuring the equipment. Default TCP port: 8080	LAN	Restricted to local network only.	Restricted to local network only/ unrestricted.
AT Command Interface on Ethernet	Used for configuring the equipment. Default EtherType: 0x0666	LAN	On	Yes

4. Preparation

4.1. Support and Resources

For additional documentation and software downloads, FAQs, troubleshooting guides and technical support, please visit www.hms-networks.com/technical-support.

TIP
Have the product article number available, to search for the product specific support web page. You find the product article number on the product cover.

4.2. Optional Equipment

Bridge II Ethernet can be mounted on a standard DIN rail using the optional DIN mounting kit.

The DIN mounting kit is not included with the Bridge II Ethernet. For information about ordering the DIN mounting kit, please visit www.hms-networks.com.

4.3. Network Environment

Ensure that you have all the necessary information about the capabilities and restrictions of your local network environment before installation.

4.4. Placement for Optimal Reception

Antenna Considerations

For models with internal antenna the characteristics of the antenna should be considered when choosing the placement and orientation of the Bridge II Ethernet.

Required Distance Between Devices

For optimal reception, wireless devices require a zone between them clear of objects that could otherwise obstruct or reflect the signal.

To avoid signal interference, a minimum distance of 50 cm between the wireless devices should be observed.

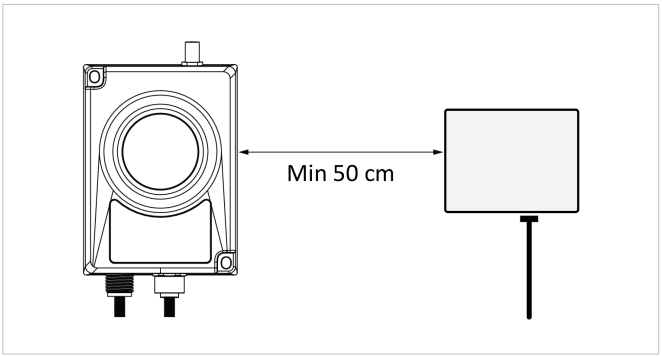


Figure 3. Required minimum distance between wireless devices

See Wireless Technology Basics (page 80).

Required Distance Between Device and Human

At least 20 cm separation distance between the device and the user’s body must be maintained at all times.

4.5. When to Use Bluetooth or WLAN

Use Bluetooth when:

- The wireless link has an Anybus Wireless Bolt or Anybus Wireless Bridge II at both ends.
- An interruption-free connection is more important than data throughput.
- Interference robustness is important, e.g. in an industrial environment.
- A Profinet I/O cycle time or EtherNet/IP RPI of 64 ms or more is acceptable.

Use WLAN when:

- Connecting to other types of wireless devices or a WLAN infrastructure.
- High data throughput speed is more important than connection reliability.
- Large file transfers are expected.
- WLAN channel frequency planning is possible.
- A low Profinet I/O cycle time or EtherNet/IP RPI is desired.

4.6. Bluetooth Limitations

Due to different implementations of Bluetooth by different manufacturers, Bluetooth PAN (Personal Area Network) may not work with some devices.

WLAN 5 GHz cannot be used at the same time as WLAN 2.4 GHz or Bluetooth.

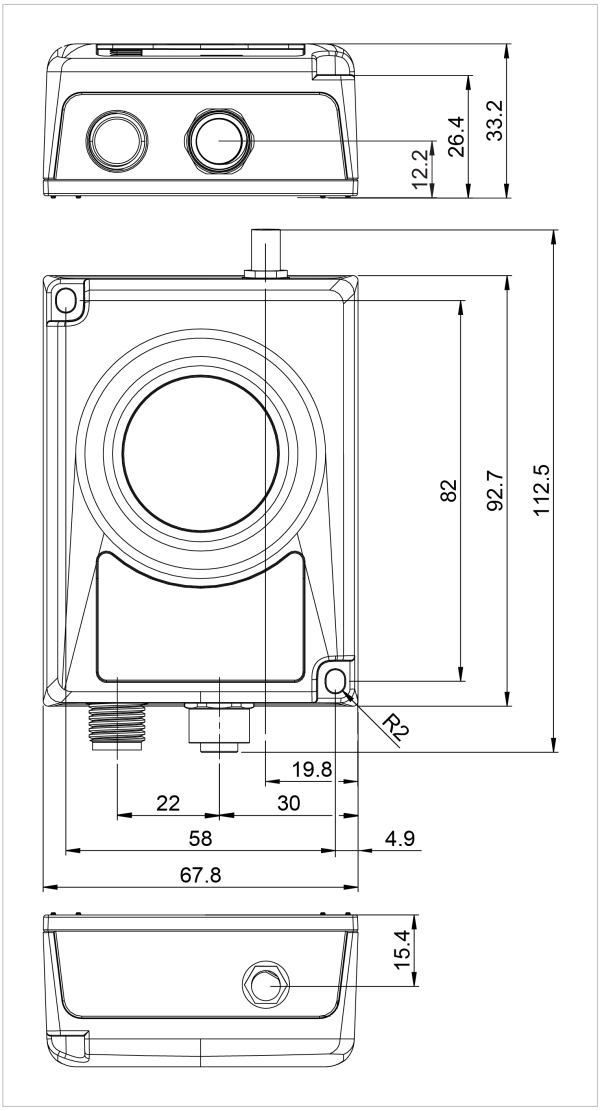
4.7. I/O-Data Cycle Time Considerations

Based on recommendations from industrial equipment suppliers, such as Rockwell and Siemens, use the following minimum I/O data cycle times for PROFINET and EtherNet/IP networks:

- Wireless link Point-to-Point with Bluetooth PANU-PANU or Wi-Fi Access Point to Station: 32 ms
- Wireless link with Access Point and up to 4 wireless clients/stations, Bluetooth or Wi-Fi: 64 ms

5. Installation

5.1. Installation Drawing



All measurements are in mm.

Figure 4. Bridge II Ethernet Installation drawing

5.2. Surface Mounting

Bridge II Ethernet can be screw-mounted directly onto a flat surface.

Before You Begin

NOTE
To avoid signal interference, a minimum distance of 50 cm between the devices should be observed.
See also Wireless Technology Basics (page 80).

Procedure

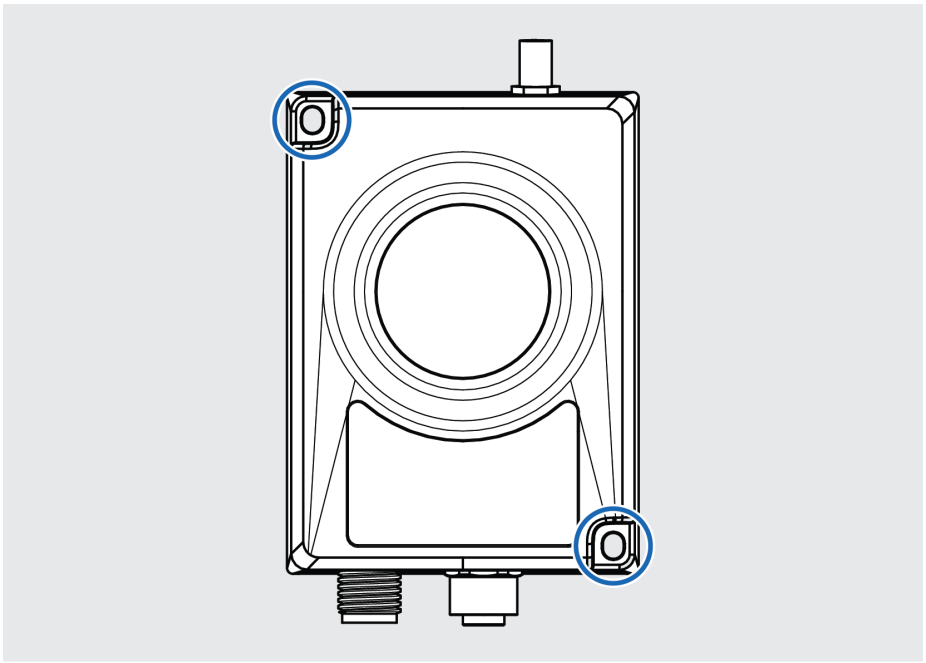


Figure 5. Surface mounting holes

To screw-mount the Bridge II Ethernet on a surface, use the two holes (Ø 4 mm) at the corners of the Bridge II Ethernet.

5.3. DIN Rail Mounting

Using the optional DIN mounting kit, Bridge II Ethernet can be mounted on a standard DIN rail. See Optional Equipment (page 8).

Before You Begin

NOTE
To avoid signal interference, a minimum distance of 50 cm between the devices should be observed. See also Wireless Technology Basics (page 80).

Procedure

To attach the Bridge II Ethernet on the DIN rail

1. Fasten the DIN clip with the 2 included screws on the rear side of the Bridge II Ethernet.

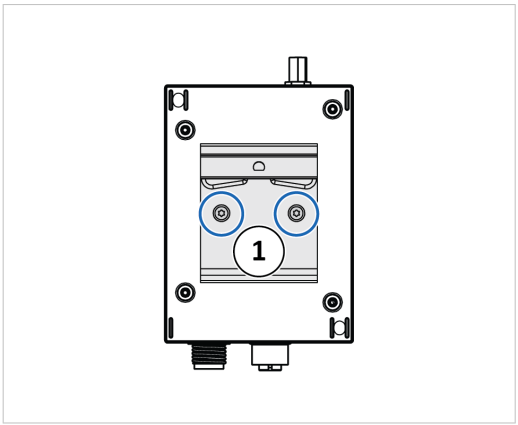


Figure 6. DIN clip on Bridge II Ethernet

2. Insert the upper end of the DIN rail clip into the DIN rail.
3. Push the bottom of the DIN rail clip into the DIN rail.

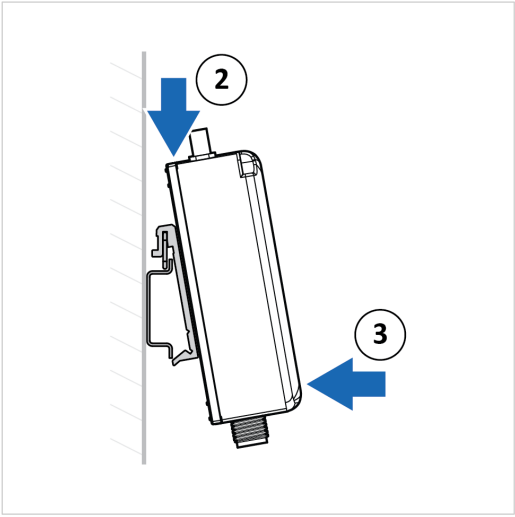


Figure 7. Attach Bridge II Etherneton DIN rail

5.4. Connect to LAN and Power

Before You Begin

CAUTION
This equipment is recommended for use in both industrial and domestic environments. For industrial environments it is mandatory to use the functional earth connection to comply with immunity requirements. For domestic environments the functional earth must be used if a shielded Ethernet cable is used, in order to meet emission requirements.

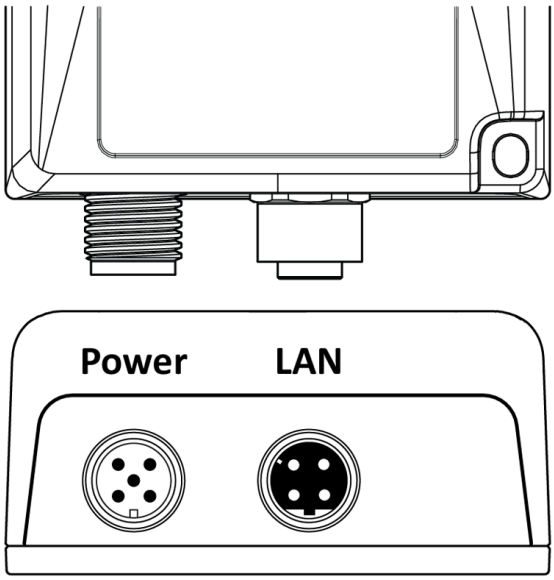
Digital Input Considerations
Digital input is used for additional functionality with advanced configurations and to remotely reset the unit.

IMPORTANT
If voltage is applied to the digital input for more that 10 seconds the unit will be reset to factory defaults.

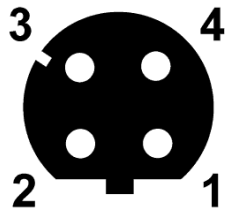
IMPORTANT
If wiring length exceeds 3 meters, signal wiring for the digital input must be carried in the same cable as power and functional earth.

For more information about digital input, visit www.hms-networks.com/technical-support.

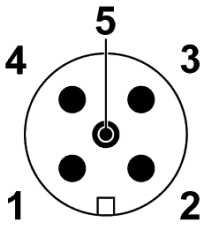
Procedure



1. Connect the Bridge II Ethernet LAN connector to a Ethernet network.

LAN Connector D-coded female M12	Pin	Function	Color coding (T568B)
	1	Transmit +	Orange/White
	2	Receive +	Green/White
	3	Transmit -	Orange
	4	Receive -	Green

2. Connect the Bridge II Ethernet power connector to a power supply.

Power Connector	Pin	Function
	1	Power + (9–30 V)
	2	Digital Input Ground
	3	Power Ground
	4	Digital Input + (9–30 V)
	5	Functional Earth

6. Configuration

6.1. Bridge II Ethernet Built-In Web Interface

The Bridge II Ethernet built-in web interface is used to configure, maintain and troubleshoot the Bridge II Ethernet. Parameters can be set individually or using pre-configured Easy Config modes.

The web interface is accessed by pointing a web browser to the IP address of the unit.

The default address is 192.168.0.99.

See also Access the Built-In Web Interface (page 17).

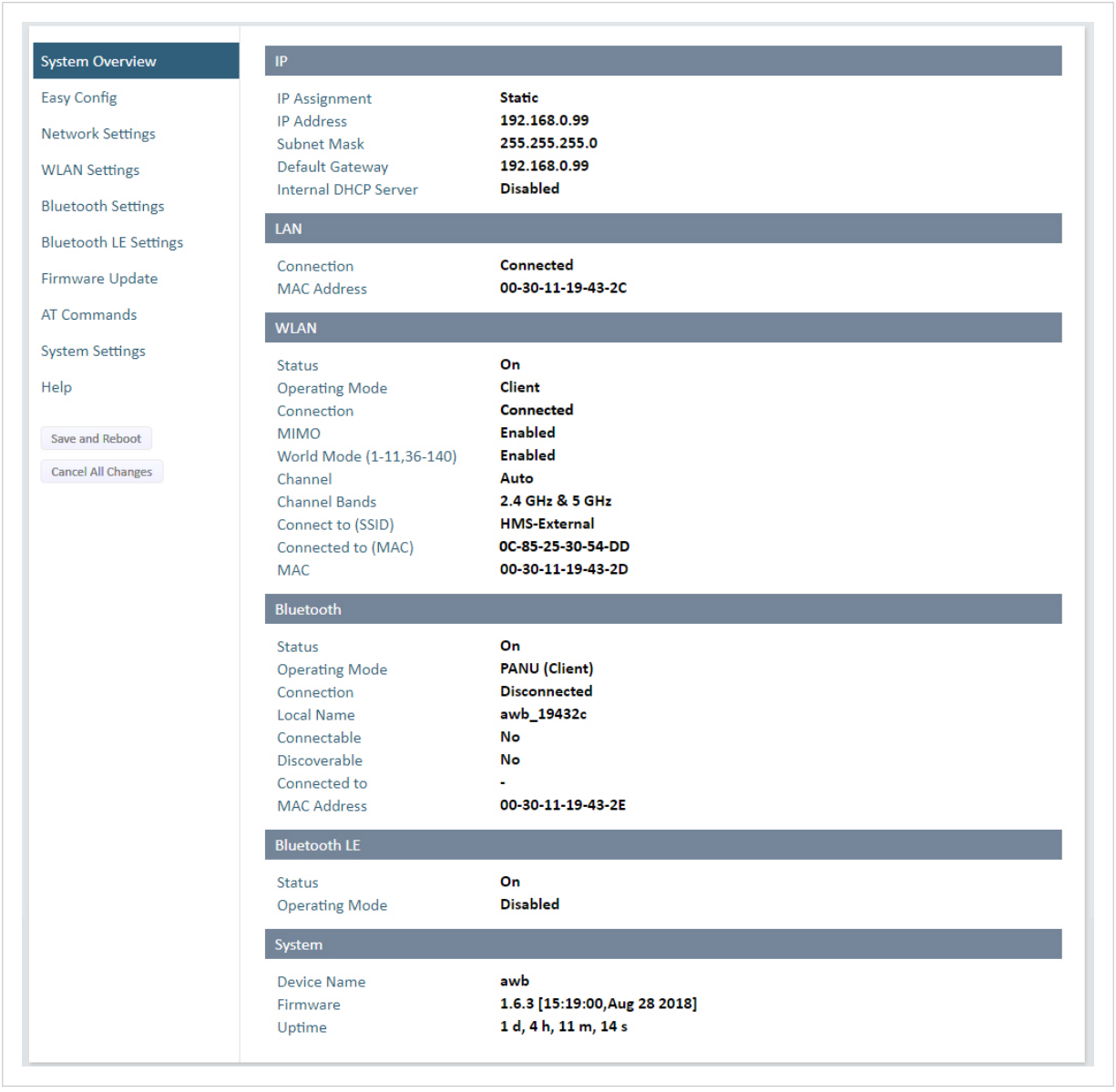


Figure 8. System Overview page example

The **System Overview** page shows current settings and network connection status.

The **Help** page describes the AT commands that can be used for advanced configuration.

6.2. Connect to Configure

Initial Setup and Factory Reset

For initial setup or after a factory reset: To configure the Bridge II Ethernet using its built-in web interface, it must be connected to a PC via an Ethernet cable.

Procedure

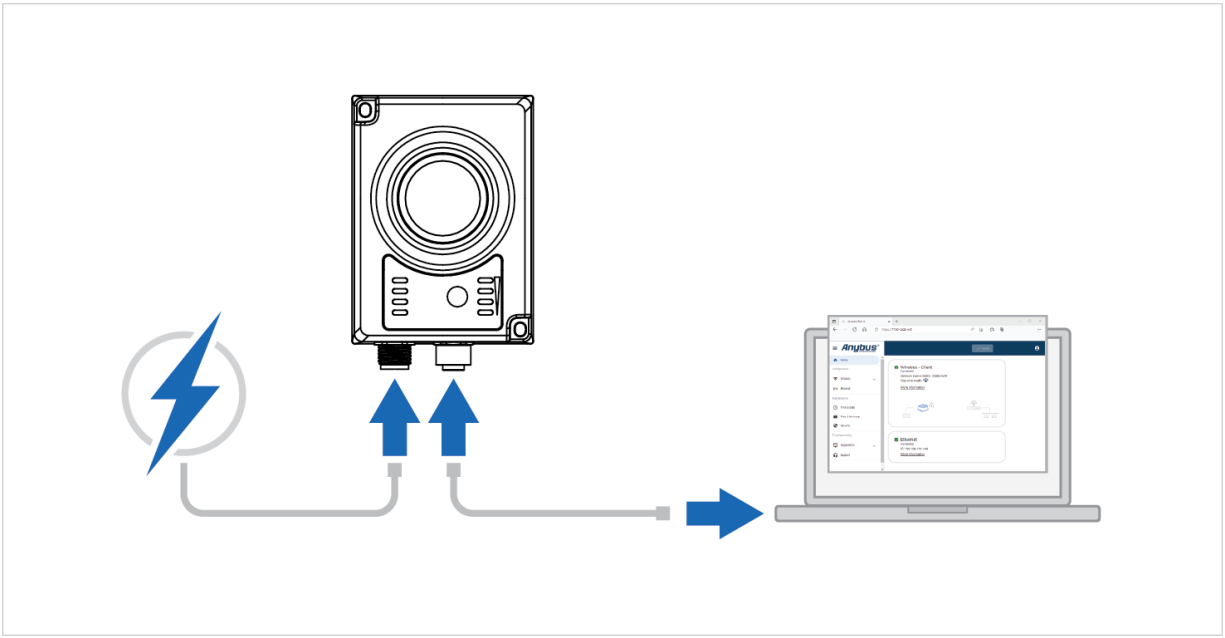


Figure 9. Connect to PC and Power

1. Connect the Bridge II Ethernet Ethernet port to your PC.
2. Connect the Bridge II Ethernet Power connector to a power supply.

When Connected to Wi-Fi Network

Once connected to a Wi-Fi network after initial setup, you can configure the Bridge II Ethernet wirelessly through the web interface — just ensure that **Local Configuration** is disabled.

See Local Configuration (page 49).

6.3. Access the Built-In Web Interface

NOTE
By default, **Local configuration** is enabled, which restricts access to the Bridge II Ethernet built-in web interface.

For a device to access the Bridge II Ethernet built-in web interface, connect it directly to the Bridge II Ethernet LAN (Local Area Network) port.

See also Local Configuration (page 49).

6.3.1. Required IP Address Settings

To be able to access the Bridge II Ethernet built-in web interface you may need to adjust the IP settings, choose one of the following methods.

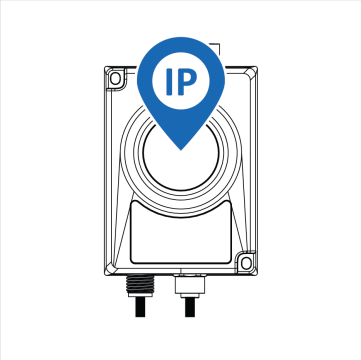
NOTE
The Bridge II Ethernet default IP address is 192.168.0.99 and the subnet mask is 255.255.255.0.

Option 1- Set a Static IP Address on Your PC

NOTE
When you change to a static IP address on your PC, internet access may be lost.

On the PC accessing the Bridge II Ethernet built-in web interface, set a static IP address within the same IP address range as the Bridge II Ethernet IP address.

Option 2 - Change the IP Address on the Bridge II Ethernet Ethernet port



Use the software application HMS IPconfig to find and change the IP address on the Bridge II Ethernet Ethernet port, to one within the same IP address range as the PC accessing the Bridge II Ethernet built-in web interface.

To download the installation files, please visit www.hms-networks.com/technical-support and enter the product article number to search for the Bridge II Ethernet support web page. You find the product article number on the product cover.

Result

Now you can enter the Bridge II Ethernet IP address in your web browser and access the built-in web interface login page.

6.3.2. Login to the Built-In Web Interface

The Bridge II Ethernet built-in web interface can be accessed from a standard web browser.

Before You Begin

> **NOTE**
> The Bridge II Ethernet default IP address is 192.168.0.99 and the subnet mask is 255.255.255.0.

Procedure

Login to the Bridge II Ethernet built-in web interface:

1. Open a web browser.
2. Click to select the **Address bar** and enter http:// and the Bridge II Ethernet IP address.

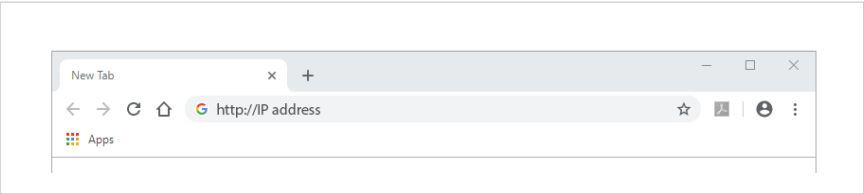


Figure 10. Enter IP address in web browser

3. Press **Enter**.
   The Bridge II Ethernet built-in web interface login screen appears.
4. Enter the **Password** and click **Sign in**.

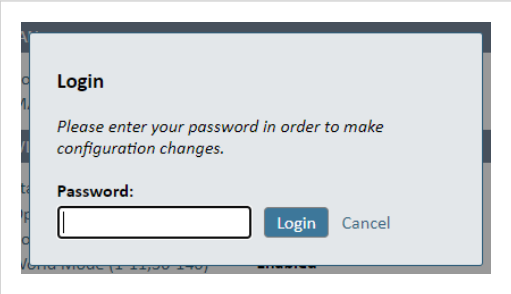


Figure 11. Built-in web interface login screen

Result

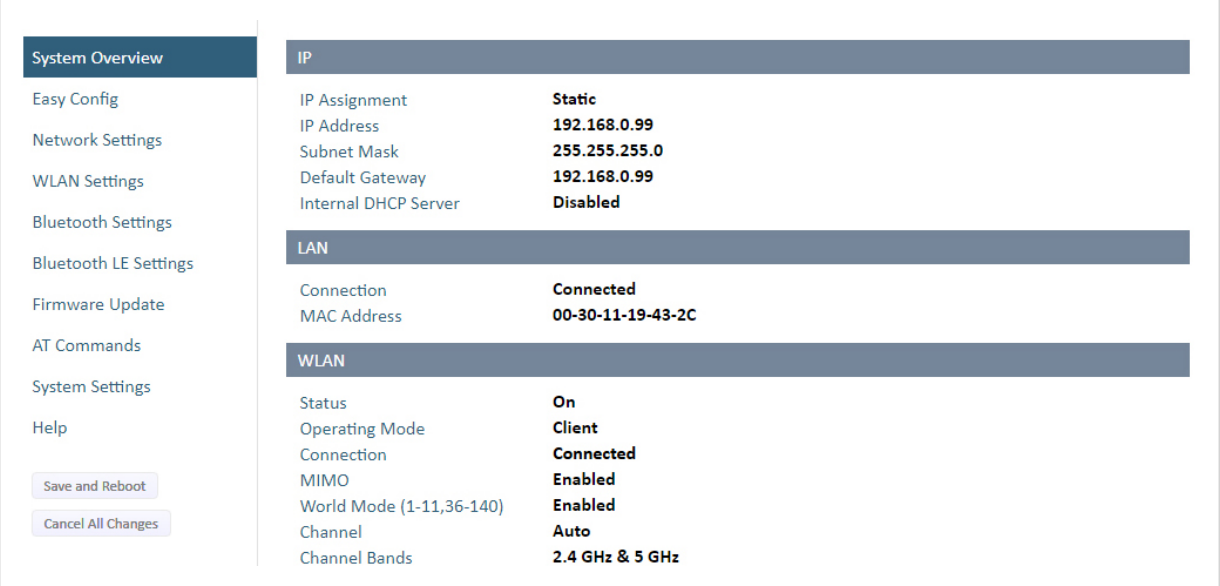
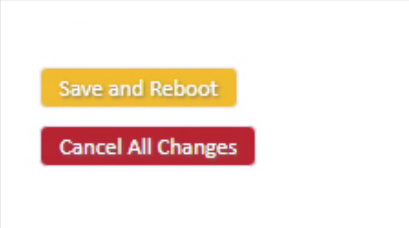


Figure 12. page

6.4. To Save and Reboot



Cancel Changes

To cancel changes, you have made to the settings:

In the left sidebar menu, click **Cancel All Changes**.

To restore settings, see Restore Settings From Backup File (page 73).

Apply Changes

To apply changes, click **Save and Reboot** in the left sidebar menu.

Bridge II Ethernet restarts for the changes to take effect.

6.5. Factory Default Settings

The Bridge II Ethernet comes with the following factory default settings.

Default Network Settings	
IP Assignment	Static
IP Address	192.168.0.99
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.99
Internal DHCP Server	Disabled
DHCP Interfaces	All

Default WLAN Settings	
Operating Mode	Client
Channel Bands	2.4 GHz & 5 GHz
Authentication Mode	WPA/WPA2–PSK
Channel	Auto
Bridge Mode	Layer 3 IP forward
MIMO	AWB3000: Enabled AWB3010: Disabled

Default Bluetooth Settings	
Operating Mode	PANU (Client)
Local Name	[generated from MAC address]
Pairing Mode	Enabled
Connectable	No
Discoverable	No
Security Mode	Just works
Bluetooth LE	Operating Mode: Disabled Connectable: No Discoverable: No

6.6. Configuration Methods

There are different methods available for configuring the Bridge II Ethernet.

Built-In Web Interface Settings

Bridge II Ethernet can be configured via the settings in the built-in web interface.

See Configure Settings in the Built-In Web Interface (page 35).

Easy Config Modes

Bridge II Ethernet can be configured using one of the pre-configured Easy Config modes.

See Configuration with Easy Config (page 22).

AT Commands

Advanced configuration can be carried out by issuing AT (modem) commands through the web interface or over a Telnet or RAW TCP connection to port 8080.

For more information about how to use the AT commands, navigate to the built-in web interface **Help** page or see the AT Commands Reference Guide.

See also Configuration with AT Commands (page 31).

6.7. Configuration with Easy Config

6.7.1. Available Easy Config Modes

Bridge II Ethernet may be configured using one of the pre-configured Easy Config modes.

NOTE

To cancel Easy Config mode 11, the unit must be reset to factory default settings. See Reset to Factory Default (page 75)

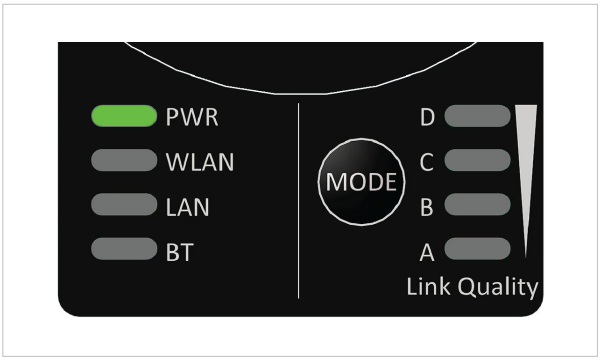


Figure 13. Easy Config A-B-C-D LED indicators

Table 1. Easy Config modes

EC	Active LED				Role	Description
1	A				Bluetooth PANU	Used for setting up point-to-point communication. The unit scans for another unit in Config Mode 4. If no connection is established within 120 seconds, the scan will be aborted and the device will return to its initial state. When a unit in mode 4 is detected: The scanning unit configures itself as a Bluetooth PANU Client, securely pairs, sends a connection configuration to the detected unit, and then restarts. The detected unit restarts and attempt to connect to the first unit as a PANU Client.
2		B			N/A	Reset configuration to factory defaults.
3	A	B			N/A	Reset IP settings to factory defaults.
4			C		Client	Configure units in mode 4 as Clients. Wait for automatic configuration. The unit listens for 120 seconds or until receiving a configuration.
5	A		C		WLAN AP	The unit scans for other units in Config Mode 4 and configure them as Clients. Timeout occur after 120 seconds. Restart as Access Point and connect Clients.
6		B	C		Bluetooth NAP	
7	A	B	C		WLAN AP	The unit scans for other units in Config Mode 4 and configure them as Clients. Timeout occur after 120 seconds. Restart as Access Point and connect Clients. Apply PROFINET optimization to all units. PROFINET messages will have priority over TCP/IP frames.
8				D	Bluetooth NAP	
9	A			D	Bluetooth PANU	Configure unit as a Client and scan for another Client (PANU to PANU). Apply PROFINET optimization to both units. The unit listens for 120 seconds or until a configuration is established.
10		B		D	(any)	Apply PROFINET optimization and restart. No other configuration settings are changed.
11	A	B		D	(any)	Enable PROFIsafe mode. The unit is locked in PROFIsafe mode. No other configuration settings are changed.

The Easy Config modes are also described when selected in the built-in web interface. See How to Activate an Easy Config Mode.

6.7.2. Easy Config Modes Time Considerations

Table 2. Easy Config modes time considerations

Mode	Timeout
1 and 9	The unit listens for 40 seconds or until a configuration is established.
4	The unit listens for 120 seconds or until receiving a configuration.
5, 6, 7 and 8	The unit scans for 120 seconds, then timeout occur.

6.7.3. Easy Config Using the MODE Button

In this topic we describe the general procedure for configuring units using the **MODE** button and Easy Config modes. For specific use case examples, see Use Cases (page 54).

Before You Begin

Default IP address settings

- The default address to Access Point unit 1 is 192.168.0.99.
- The default IP address to Client unit 1 is 192.168.0.100.

Configuration Steps

1. Power on the first Unit.

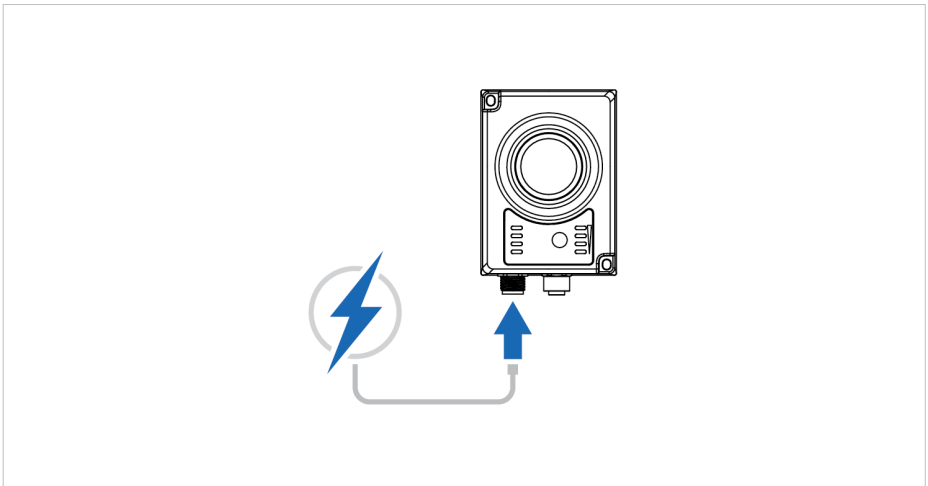


Figure 14. Connect to power

The power **PWR** LED light is lit.

2. When the Link Quality LEDs lights up and goes out again, immediately press and release **MODE**.

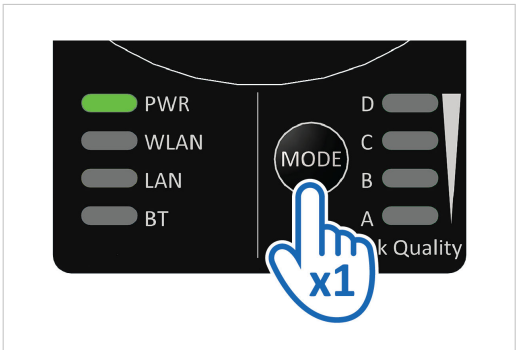


Figure 15. Press and release **MODE**

3. To select an Easy Config mode:
   a. Press **MODE** repeatedly, to cycle through the Easy Config modes.

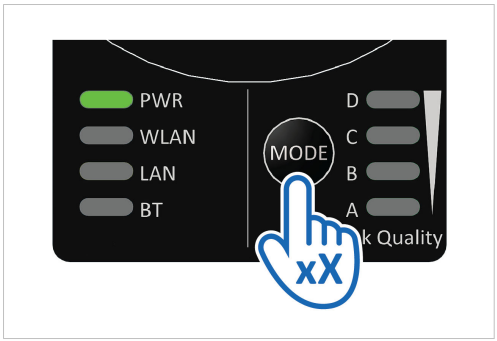


Figure 16. Select the desired mode

   b. When the **A-B-C-D** LEDs lights indicate the desired Easy Config mode, release the **MODE** button.

Table 3. Easy Config modes and LED indications

EC	LED				Role	Description
1	**A**				Bluetooth PANU	Configure as a Client and scan for another Client (PANU to PANU). Used for setting up point-to-point communication. Timeout after 120 seconds.
4			**C**		Client	Wait for automatic configuration. Timeout occur after 120 seconds.
5	**A**		**C**		WLAN AP	Configure units in mode 4 as clients. Restart as Access Point and connect Clients. Timeout occur after 120 seconds.
6		**B**	**C**		Bluetooth NAP	
7	**A**	**B**	**C**		WLAN AP	Configure units in mode 4 as clients. Restart as Access Point and connect Clients. Apply PROFINET optimization to all units. Timeout occur after 120 seconds.
8				**D**	Bluetooth NAP	
9	**A**			**D**	Bluetooth PANU	Configure as a Client and scan for another Client (PANU to PANU). Apply PROFINET optimization to both units. Timeout after 120 seconds.

4. To confirm the Easy Config mode, press and hold **MODE** for 2 seconds and then release it.

> **NOTE**
> You must confirm the Easy Config mode within 20 seconds.

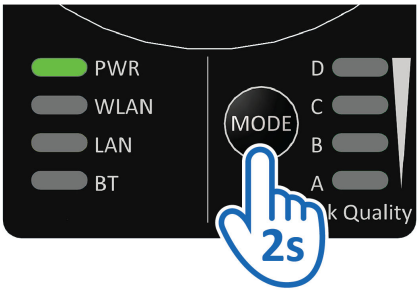


Figure 17. Confirm Easy Config mode

5. The LED lights indicating the active Easy Config mode flashes while the unit is scanning for a second unit to configure.
   Depending on the selected Easy Config mode, the following happens:

   • Easy Config mode 1 or 9: The unit restarts as a Client and starts scanning for a second unit to configure.

- Easy Config mode 4: The unit listens for 120 seconds for receiving a configuration.
- Easy Config mode 5, 6, 7 or 8: The unit restarts as an Access Point and starts scanning for a second unit to configure.

Confirm Connection

For cybersecurity reasons, the following steps are implemented to ensure the correct devices are connected:

1. The Link Status LED indicators on each unit first blink to indicate that Easy Config mode is running.
2. When Unit 1 has discovered Unit 2, the Link Status LED indicators on both units start to blink a 5x4 LED pattern in a loop.
3. Compare the units to ensure that the LED indicators flash in the same pattern.

- To allow Unit 2 to connect to Unit 1, press the **MODE** button once on each unit.

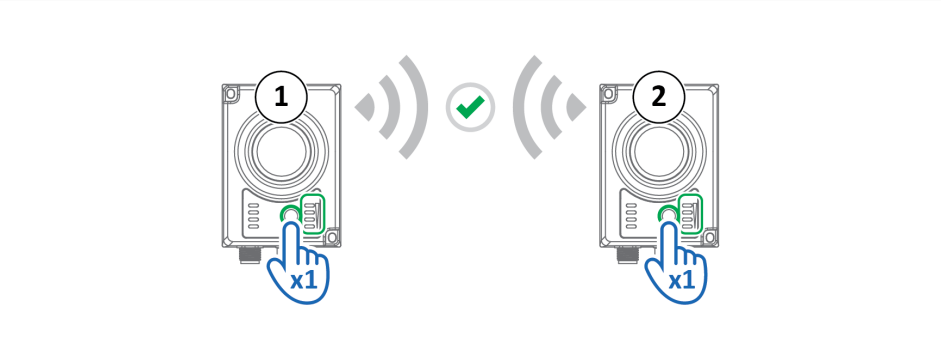


Figure 18. Codes match, Accept

- If Unit 2 detects a device other than the Bridge II Ethernet Unit 1, wait for the Easy Config mode to time out. Do not press the **MODE** button during this process.
  Ensure that no other nearby Bluetooth devices are in pairing mode, then redo the Easy Config procedure.

Figure 19. LED indicators blink on one unit only, wait for the Easy Config mode to timeout

- If the LED indicators blinking patterns do not match on both units, wait for the Easy Config mode to time out. Do not press the **MODE** buttons during this process.
  Verify that there are no unauthorized or potentially harmful devices in the area, then redo the Easy Config procedure.

Figure 20. LED indicators blinking patterns do not match, wait for the Easy Config mode to timeout

Add Additional Units
When using Easy Config Mode 5 or 6, up to seven additional Units can be added.

NOTE
When using Easy Config mode 4, the next unit to be added must be set up within 120 seconds after the first unit was restarted.

Each new Client unit will be assigned the next free IP address in the current Ethernet subnet.

To add a Unit, repeat the configuration steps.

Verify Operation

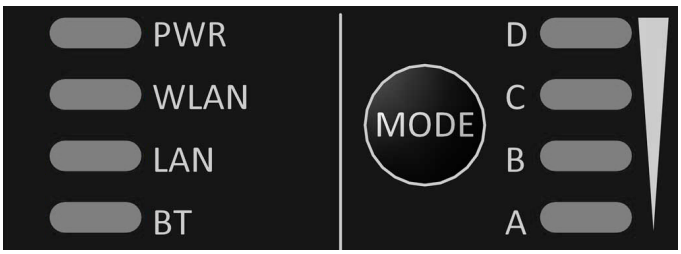


Figure 21. Status LED indicators

- On Units configured with Bluetooth, verify that the **BT** LED is lit.
- On Units configured with Easy Config Mode 4, the **A-B-C-D** LEDs lights indicates the Bluetooth link quality.
- On Units configured with WLAN, verify that the **WLAN** LED is lit.

See LED Indicators (page 51).

Configure Additional Settings
To configure additional settings, log in to the built-in web interface for each unit you want to configure.

See Configure Settings in the Built-In Web Interface (page 35)

6.7.4. Easy Config Using the Built-In Web Interface

In this topic we describe the general procedure for configuring units using the Bridge II Ethernet built-in web interface and Easy Config modes. For specific use case examples, see Use Cases (page 54).

Configuration Steps

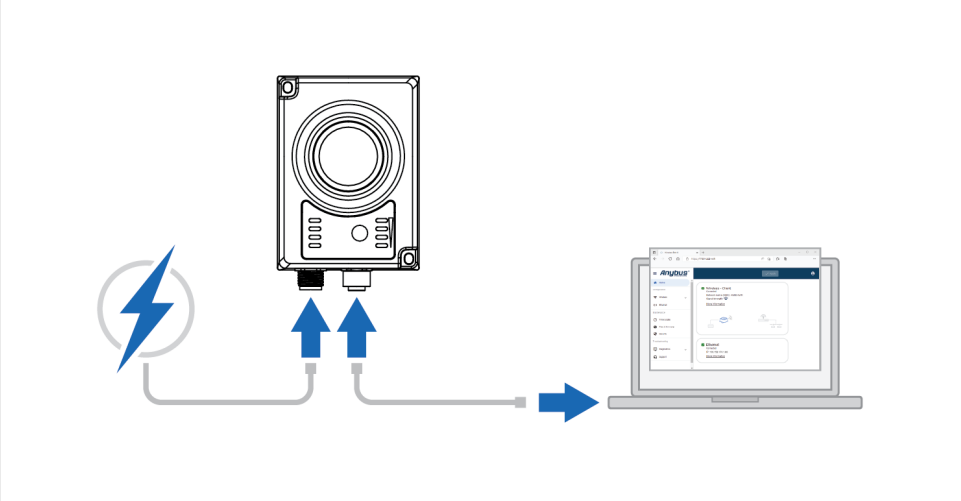


Figure 22. Connect to PC and power

1. Connect the LAN port on the first Unit to your PC.
2. Power on the first Unit.
   The power **PWR** LED light is lit.

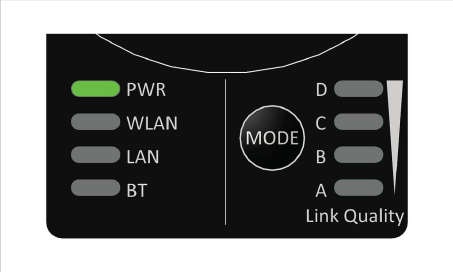


Figure 23. PWR LED

3. Login to the Built-In Web Interface of Unit 1.
4. On the **Easy Config** page, select the desired Easy Config mode from the **Select Easy Config** drop-down menu.

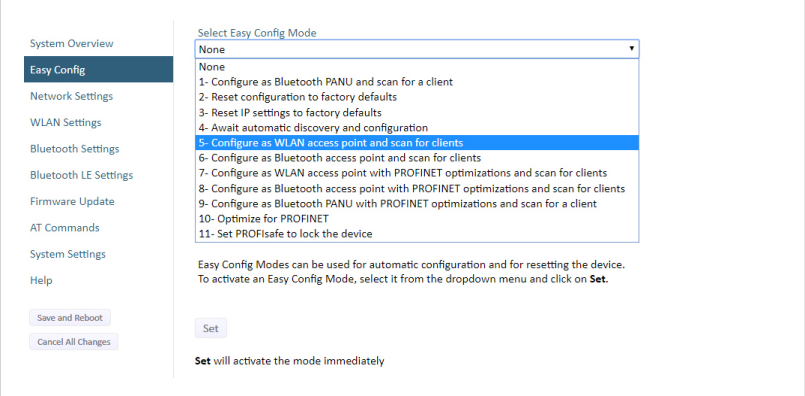


Figure 24. Easy Config Modes menu

5. Click **Set**.
   The Easy Config mode is activated immediately.

> **NOTE**
> Keep the **Easy Config** page open while the scan is in progress. Closing or leaving this page will interrupt the process.

Confirm Connection

When using one of the Easy Config Modes to connect two units, you need to confirm the connection between them.

For cybersecurity reasons, the following steps are implemented to ensure the correct devices are connected:

1. On the **Easy Config** page for each unit, a dialog window appears showing an **Easy Config confirmation** code.

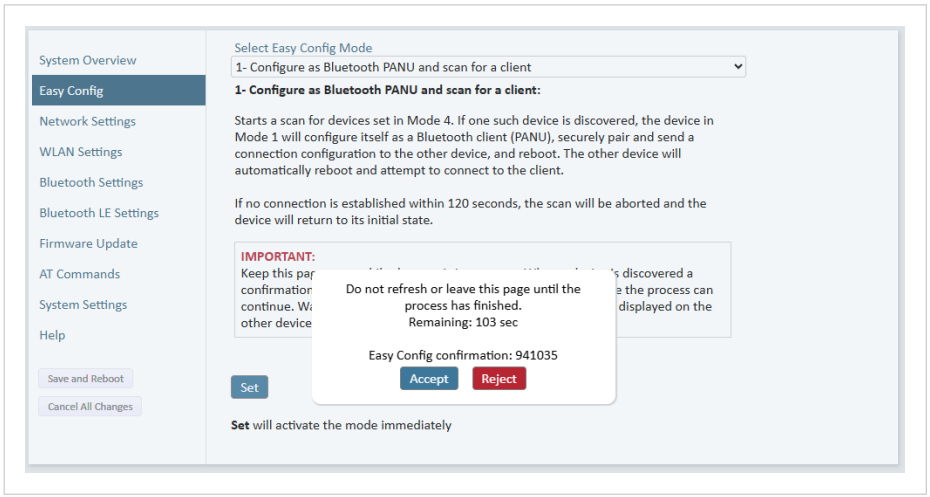


Figure 25. Easy Config page, confirmation dialog window

2. Compare the codes displayed in the dialog windows of both units to ensure they are identical.

- To allow Unit 2 to connect to and configure Unit 1, click **Accept** for each unit.

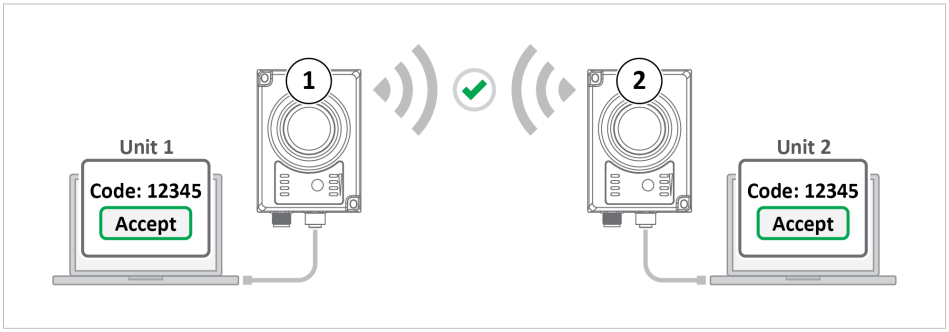


Figure 26. Codes match, Accept

- If Unit 2 detects a device other than the Bridge II Ethernet Unit 1, the dialog window appears only on Unit 2. Then, click **Reject**.
  Ensure that no other nearby Bluetooth devices are in pairing mode, then redo the Easy Config procedure.

Figure 27. Code appear for one unit only, Reject

- If the codes do not match, click **Reject** for each unit.
  Verify that there are no unauthorized or potentially harmful devices in the area, then redo the Easy Config procedure.

Figure 28. Codes do not match, Reject

Add Additional Units

When using Easy Config Mode 5 or 6, up to seven additional Units can be added.

> **NOTE**
> When using Easy Config mode 4, the next unit to be added must be set up within 120 seconds after the first unit was restarted.

Each new Client unit will be assigned the next free IP address in the current Ethernet subnet.

To add a Unit, repeat the configuration steps.

Verify Operation

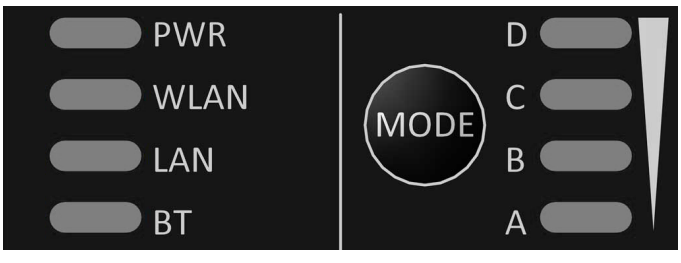


Figure 29. Status LED indicators

- On Units configured with Bluetooth, verify that the **BT** LED is lit.
- On Units configured with Easy Config Mode 4, the **A-B-C-D** LEDs lights indicates the Bluetooth link quality.
- On Units configured with WLAN, verify that the **WLAN** LED is lit.

See LED Indicators (page 51).

Configure Additional Settings

To configure additional settings, log in to the built-in web interface for each unit you want to configure.

See Configure Settings in the Built-In Web Interface (page 35)

6.8. Configuration with AT Commands

Advanced configuration can be carried out by issuing AT commands via the web interface or over a Telnet or RAW TCP connection to port 8080 or over serial interface.

Use AT commands to setting advanced parameters, that are not accessible in the Bridge II Ethernet built-in web interface.

AT commands can be used to read out parameters in text format and for batch configuration using command scripts.

For a complete list of supported AT commands, click **Help** in the built-in web interface. See also the AT Commands Reference Guide at www.hms-networks.com/technical-support.

Procedure

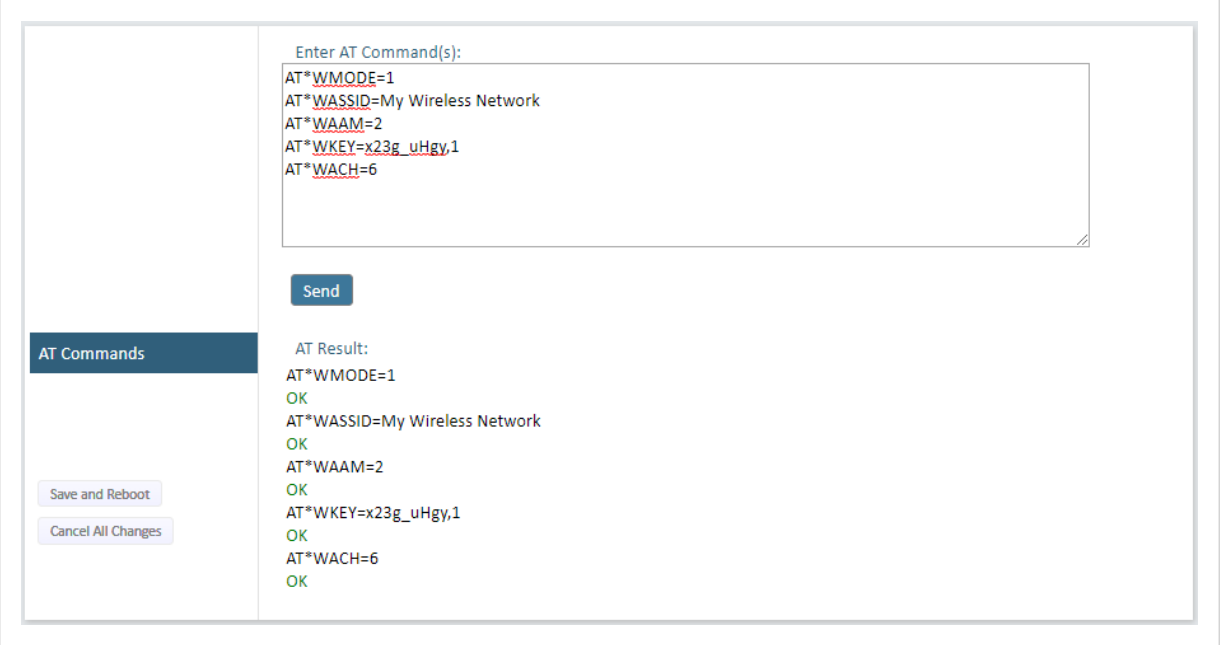


Figure 30. AT Commands and AT Results

1. Enter or paste the AT commands into the **Enter AT Command(s)** text field.
2. Click **Send**.
3. The result codes are displayed in the **AT Result** panel.

6.8.1. Enable Fast Roaming with AT Commands

Fast Roaming is only used for Client Mode.

Fast Roaming is enabled as default but can be permanently disabled using AT commands.

Procedure

Enable or Disable Fast Roaming.

1. To Enable or Disable Fast Roaming, change the value of register **4004**.
   - Enable Fast Roaming:

     ```
     ATS4004=1
     ```

   - Disable Fast Roaming:

     ```
     ATS4004=0
     ```

2. For the command to take effect, reboot the Bridge II Ethernet.
   Send the Reboot device AT Command:

   ```
   AT*AMREBOOT
   ```

For more information about how to set up WLAN roaming, see the AT Commands Reference Guide or the **Help** page in the built-in web interface.

6.8.2. Add Additional WLAN Channels with AT Commands

WLAN Channels and World Mode is only used for Client Mode.

World Mode can be disabled and additional channels added using AT commands.

NOTE
When World Mode is disabled and additional channels are used, WLAN communication may take a longer time to establish during startup.

When using additional channels:

- The unit will search for country information during the scan.
- If the scan indicates that the unit is operating within either the European (ETSI) or North American (FCC) regulatory domains, the additional channels will be enabled.
- A new scan will be performed every hour to update the regulatory domain.
- If no country information or conflicting information is detected, the unit will revert to World Mode. The unit must then be restarted to update the regulatory domain.

For more information about how to use AT commands, see the AT Commands Reference Guide or the **Help** page in the web interface.

For information on possible channels to include, see WLAN Channels and World Mode (page 40).

Procedure

Enable or Disable World Mode and add WLAN channels.

1. To Enable or Disable World Mode.
   - Enable World Mode

     ```
     AT*WMM=1
     ```

   - Disable World Mode:

     ```
     AT*WWM=0
     ```

2. To include WLAN channels for connection and roaming, use the AT Command **AT*WSCHL=<channel_list>,<store>**.

Example 1. Add 2.4 GHz channels

2.4 GHz system with Access Points in channel 1, 6 and 11. There is no 5 GHz channels.

```
AT*WSCHL=1,6,11,1
```

Example 2. Add both 2.4 GHz and 5 GHz channels

2.4 GHz channels: 1, 6 and 11

5 GHz channels: 36, 40, 44, 48

```
AT*WSCHL=1,6,11,36,40,44,48,1
```

3. For the change to take effect, reboot the Bridge II Ethernet.
   Send the Reboot device AT Command:

```
AT*AMREBOOT
```

6.8.3. To Use Bluetooth LE With AT Commands

For information about using Bluetooth LE, refer to the AT Commands Reference Guide or the **Help** page in the built-in web interface.

6.9. Configure Settings in the Built-In Web Interface

6.9.1. Network Settings

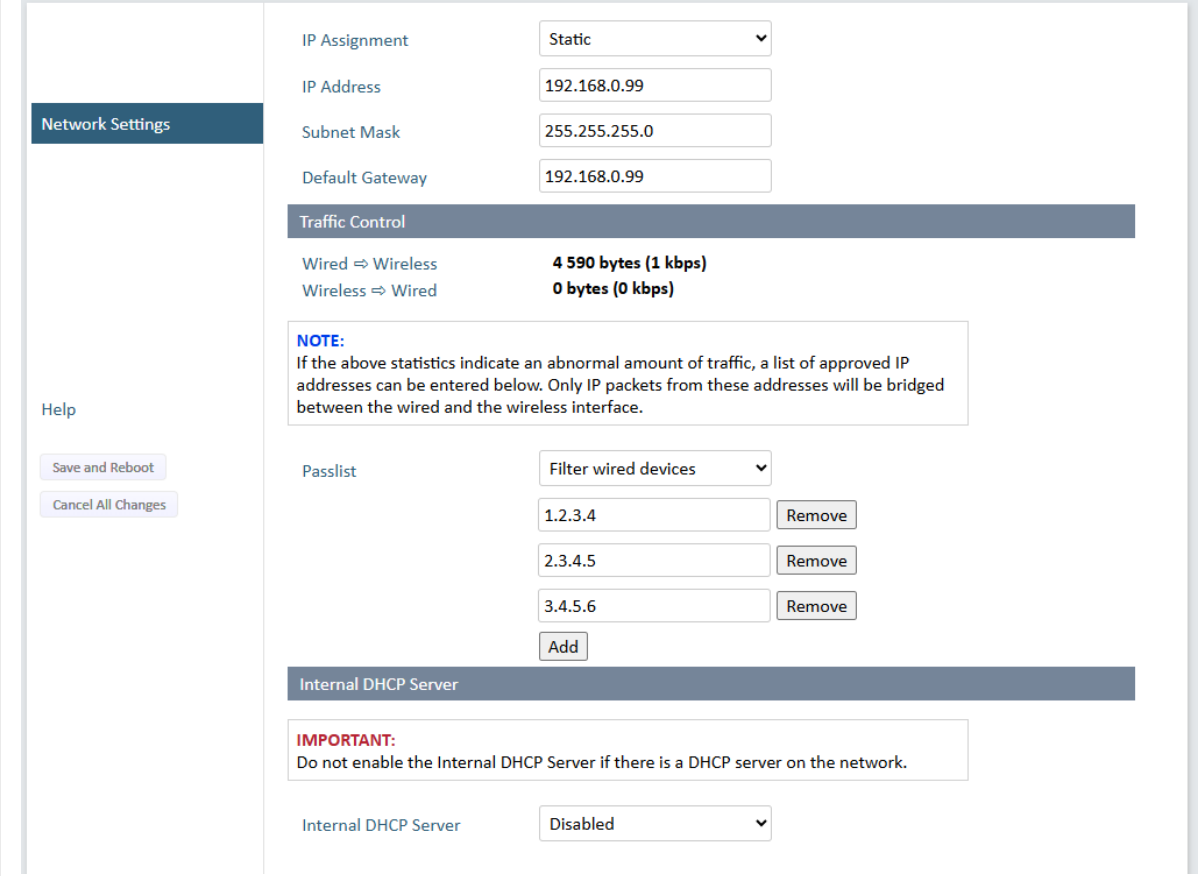


Figure 31. Network Settings page

Setting	Description
IP Assignment	Select static or dynamic IP addressing (DHCP).
IP Address	Static IP address for the unit. When you click **Save and Reboot**, the browser is redirected to the new address (not supported by all browsers).
Subnet Mask	Subnet mask when using static IP.
Default Gateway	Default gateway when using static IP.
Traffic Control	**Wired to Wireless** and **Wireless to Wired** Bytes Counter: Used to monitor and measure the amount of data being received and transmitted by the Bridge II Ethernet. Pass list: Used to specify which IP addresses have access to the Bridge II Ethernet.
Internal DHCP Server	**Disabled**: No internal DHCP functionality. **DHCP Relay Enabled**: The unit can receive a DHCP request on one interface and resend it to a DHCP server located on one of the other interfaces. Only a single DHCP server can be active for all the connected interfaces. If WLAN is used, the forwarding mode must be set to Layer 3 IP Forward. **DHCP Server Enabled**: Activates an internal DHCP server. This option is only available when IP Assignment is set to Static. To avoid IP address conflict if a DHCP server is already active on the network, use the DHCP Interfaces setting to limit the internal DHCP server to the correct interface.
DHCP Interfaces	The DHCP Interfaces function is available when **Internal DHCP Server** > **DHCP Server Enabled** is selected. **All**: By default, the DHCP Interfaces function is set to use all interfaces. **Wired Ethernet**: The internal DHCP server only listens for clients on the wired Ethernet interface.

Setting	Description
	Wireless Interfaces: The internal DHCP server listens for clients on all supported wireless interfaces (WLAN/ Bluetooth).
Start Address (Y)	The internal DHCP server will assign up to 7 IP addresses starting from **X.X.X.Y**. **X** is taken from the current static IP address setting, and Y is the value in **Start Address**. Already allocated addresses will be skipped, including the address of the unit itself. The subnet mask setting is ignored.
	Example 3. Start address examples IP Address: 192.168.0.99, Start Address: 101 DHCP range = 192.168.0.101 – 192.168.0.107 IP Address: 192.168.0.103, Start Address: 101 DHCP range = 192.168.0.101 – 192.168.0.108 7 addresses are allocated but the address of the unit is skipped.

6.9.2. Traffic Control

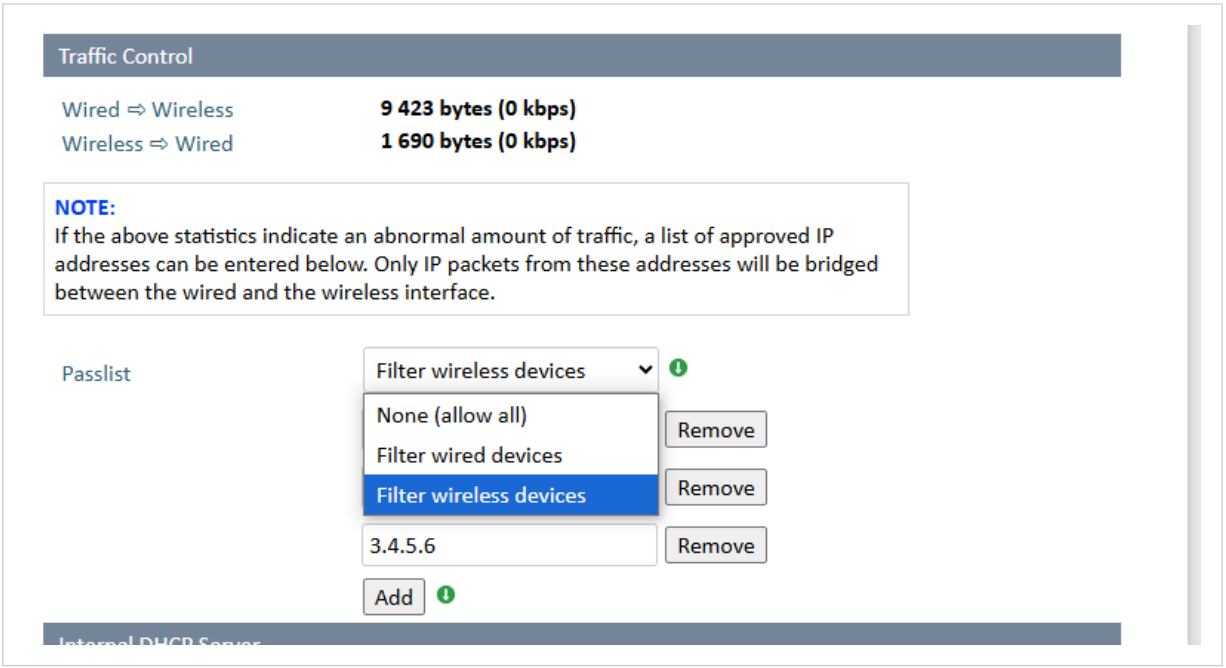


Figure 32. Network Settings, Traffic Control

Bytes Counter

> **IMPORTANT**
> Monitoring unusual traffic patterns can help detect potential security threats and identify unauthorized data transfers or potential intrusions.

Use the byte counter to monitor and measure the amount of data being received and transmitted by the Bridge II Ethernet.

Passlist

> **IMPORTANT**
> A pass list is used to specify which IP addresses have access to the connected network.
>
> Only IP traffic from sources on the passlist is allowed; all other IP traffic is blocked.
>
> Other Ethernet traffic, such as PROFINET over Layer 2, is still bridged from the Bridge II Ethernet.
>
> Restricting access to only trusted sources can help improve security.

By default all traffic is permitted, **Traffic Control None (allow all)** is selected.

Procedure

1. From the **Passlist** menu, select:
   - **Filter wired devices**, to filter devices connected to the Bridge II Ethernet via Ethernet.
   - **Filter wireless devices**, to filter devices wirelessly connected to the Bridge II Ethernet.
2. In the input field, enter the trusted IP address.
3. To add more sources, click **Add**.
   You can add up to 5 sources.

6.9.3. Layer 3 IP Forward Connectivity Considerations

When using **Layer 3 IP forward** in an enterprise network, such as a Cisco Wireless LAN Controller, the connectivity may be reduced.

The cause may be:

- Multiple devices sharing a single wireless interface is not typically supported without special configuration.
- The network cannot enforce a 1-to-1 mapping of IP to MAC addresses and must allow propagation of broadcasted ARP messages over the wireless segment in order to route traffic to the bridged devices.
  If this for security or performance reasons is not acceptable, a setup with a single Ethernet node connected to the Wireless Bridge is recommended.

6.9.4. WLAN Settings General

Figure 33. WLAN Settings page

Setting	Description
Enable	Enable/disable the WLAN interface.
Operating Mode	Choose operation as WLAN **Client** or **Access Point**. When **Access Point** is selected, additional settings will be available.
Channel Bands	**NOTE** The unit can be configured to scan on both the 2.4 GHz and 5 GHz channel bands but can only communicate on one band at a time. Choose to scan only the 2.4 GHz or 5 GHz channel band, or both (default).

6.9.5. WLAN Settings for Client

Figure 34. WLAN Settings page

Connect to settings for Client

Setting	Description
Scan for Networks	To scan the selected frequency band(s) for discoverable WLAN networks, click **Scan for Networks**. Select a network from the drop-down menu to connect to it.
Connect to SSID	To connect manually to a network, enter its SSID (network name) here. This can be used if the network does not broadcast its SSID.
Authentication Mode	Select the authentication/encryption mode required by the network, **Open**, **WEP64/128**, or **WPA/WPA2-PSK**. **Open**: Not secure. No password or encryption is used. **WEP64/128**: Basic security. Use only if needed for compatibility with legacy devices. **WPA/WPA2-PSK**: Recommended for most networks. WPA2 is more secure than WPA.
Passkey	When using **WPA/WPA2-PSK** or **WEP64/128**, enter the passkey.

6.9.6. WLAN Roaming

Bridge II Ethernet supports Fast Roaming according to IEEE 802.11r.

This enables a WLAN Client to roam quicker between WLAN Access Points that have the same SSID and support IEEE 802.11r.

See also Enable Fast Roaming with AT Commands (page 32).

6.9.7. WLAN Channels and World Mode

WLAN Channels and World Mode is only used for Client Mode.

NOTE
The maximum output power will be reduced on some channels depending on regulatory requirements.

Which channels are available for WLAN communication is restricted by the regulatory domain where the unit is operating.

Bridge II Ethernet supports regulatory domain detection and channel settings for FCC and ETSI according to the IEEE 802.11d specification.

6.9.8. WLAN Settings for Access Point

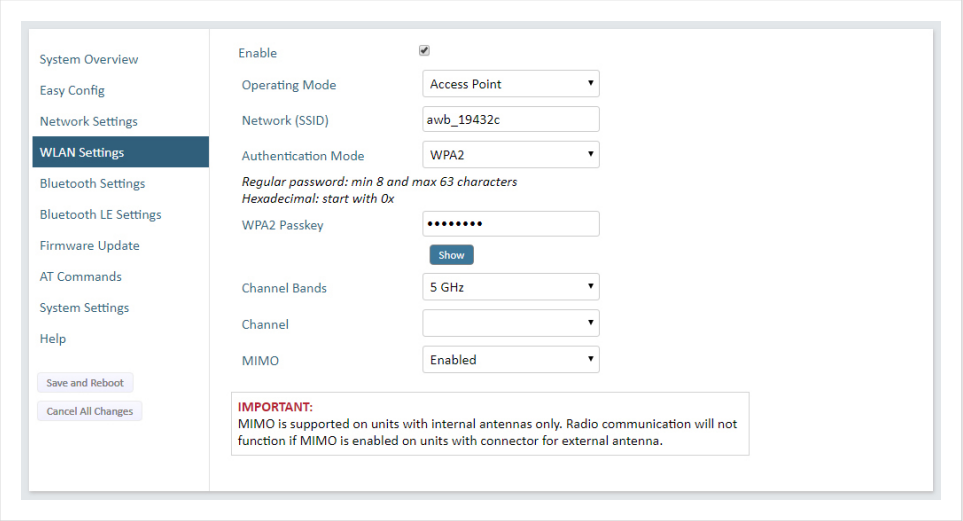


Figure 35. WLAN Settings page

Connect to settings for Access Point

The following settings are specific for Access Point mode:

Setting	Description
Network (SSID)	Enter an SSID (network name) for the Bridge II Ethernet. If this entry is left blank, the unit will generate an SSID which includes the last 6 characters of the MAC ID.
Authentication Mode	Select the authentication/encryption mode to use for the Access Point. When **Open** is selected there is no encryption or authentication. When **WPA2** is selected WPA2 PSK authentication with AES/CCMP encryption is used.
WPA2 Passkey	Enter a string in plain text or hexadecimal format to use for authentication. Regular (plain text) passwords must be between 8 and 63 characters. All characters in the ASCII printable range (32–126) are allowed, except " (double quote) , (comma) and \ (backslash). Hexadecimal passwords must start with 0x and be exactly 64 characters. See WPA2 Password Examples (page 41).
Channel Bands, Channel	Select the WLAN channel band and channel to use for the Access Point. Valid channels are 1 to 11 for the 2.4 GHz band and 36, 40, 44, 48 for the 5 GHz band.

WPA2 Password Examples

IMPORTANT
Do not use the example passwords in a live environment!

Example 4. Plain text password

For plain text passwords a combination of upper and lower case letters, numbers, and special characters is recommended.

Example of a strong plain text password: **uS78_xpa&43**

Example 5. Hexadecimal password example

```
0x000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f
```

6.9.9. WLAN Advanced Settings

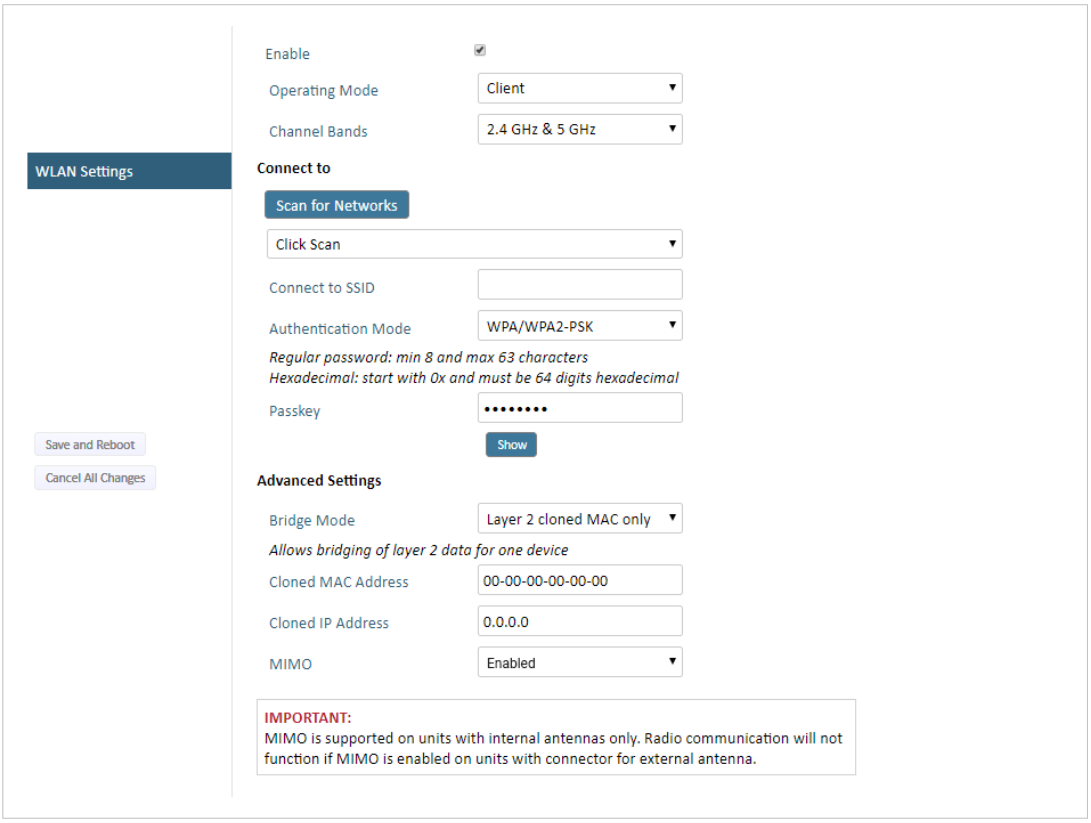


Figure 36. WLAN Settings page

Advanced Settings

Setting	Description
Bridge Mode	**Layer 2 tunnel**: All layer 2 data will be bridged over WLAN. Use when multiple devices on both sides of an Ethernet network bridge must be able to communicate via WLAN (many-to-many). Only works between Anybus Wireless Bolt or Wireless Bridge II devices. **Layer 2 cloned MAC only**: Layer 2 data from only a single MAC address (specified below) will be bridged over WLAN (many-to-one). **Layer 3 IP forward**: Default setting. IP data from all devices will be bridged over WLAN. This mode must be used when using the DHCP Relay function. See Layer 3 IP Forward Connectivity Considerations (page 38).
Cloned MAC Address	The MAC address to use with **Layer 2 cloned MAC only**.
Cloned IP Address	The IP address to use with **Layer 2 cloned MAC only**.
MIMO	MIMO (multiple input, multiple output) antenna technology uses multiple antennas for wireless communication in 802.11n. **IMPORTANT** MIMO is supported on units with internal antennas only. Radio communication will not function if MIMO is enabled on units with connector for external antenna.

6.9.10. Bluetooth Settings General

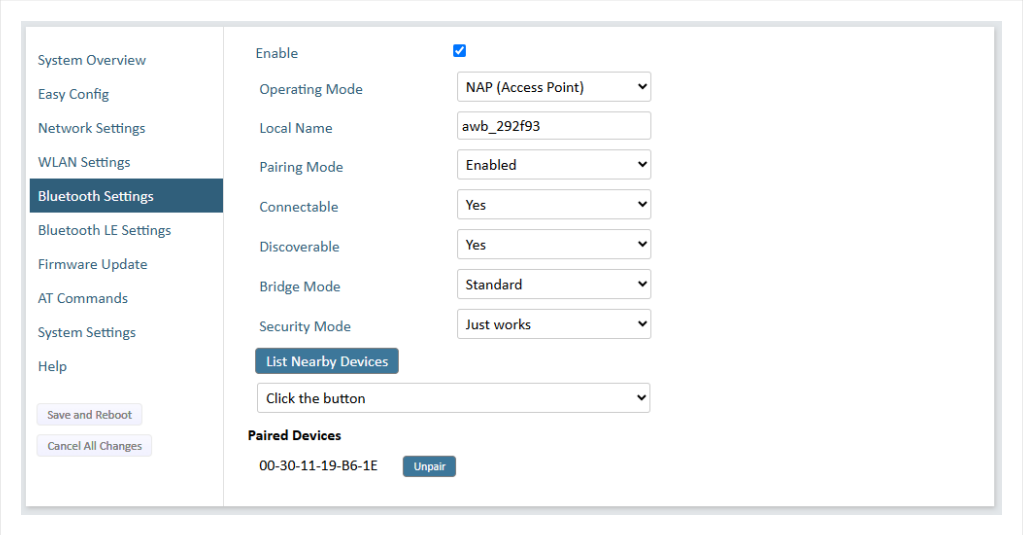


Figure 37. Bluetooth Settings page

General settings

Setting	Description
Enable	Enable/disable the Bluetooth interface.
Operating Mode	**PANU (Client)**: The unit will operate as a Bluetooth PAN (Personal Area Network) User device. It can connect to another single Bluetooth PANU device or to a Bluetooth Network Access Point. **NAP (Access Point)**: The unit will operate as a Bluetooth Network Access Point. It can connect to up to 7 Bluetooth PANU devices.
Local Name	Identifies the unit to other Bluetooth devices. If left blank, the unit will use a default name including the last 6 characters of the MAC ID.
Pairing Mode	**Enabled**: The Bridge II Ethernet allows other Bluetooth devices to pair with it. **Disabled**: The Bridge II Ethernet does not allow other Bluetooth devices to pair with it.
Connectable	Enable to make the unit accept connections initiated by other Bluetooth devices.
Discoverable	Enable to make the unit visible to other Bluetooth devices.

Connect to settings

Setting	Description
Security Mode	**Disabled**: No encryption or authentication. **PIN**: Encrypted connection with PIN code security. This mode only works between two units of this type and brand (not with third-party devices). PIN codes must consist of 4 to 6 digits. **Just Works**: Encrypted connection without PIN code.

Paired devices

The Bluetooth MAC addresses of the connected devices are listed in the **Paired devices** panel.

To unpaire a devices, click **Unpaire**.

6.9.11. Bluetooth Settings for PANU Mode

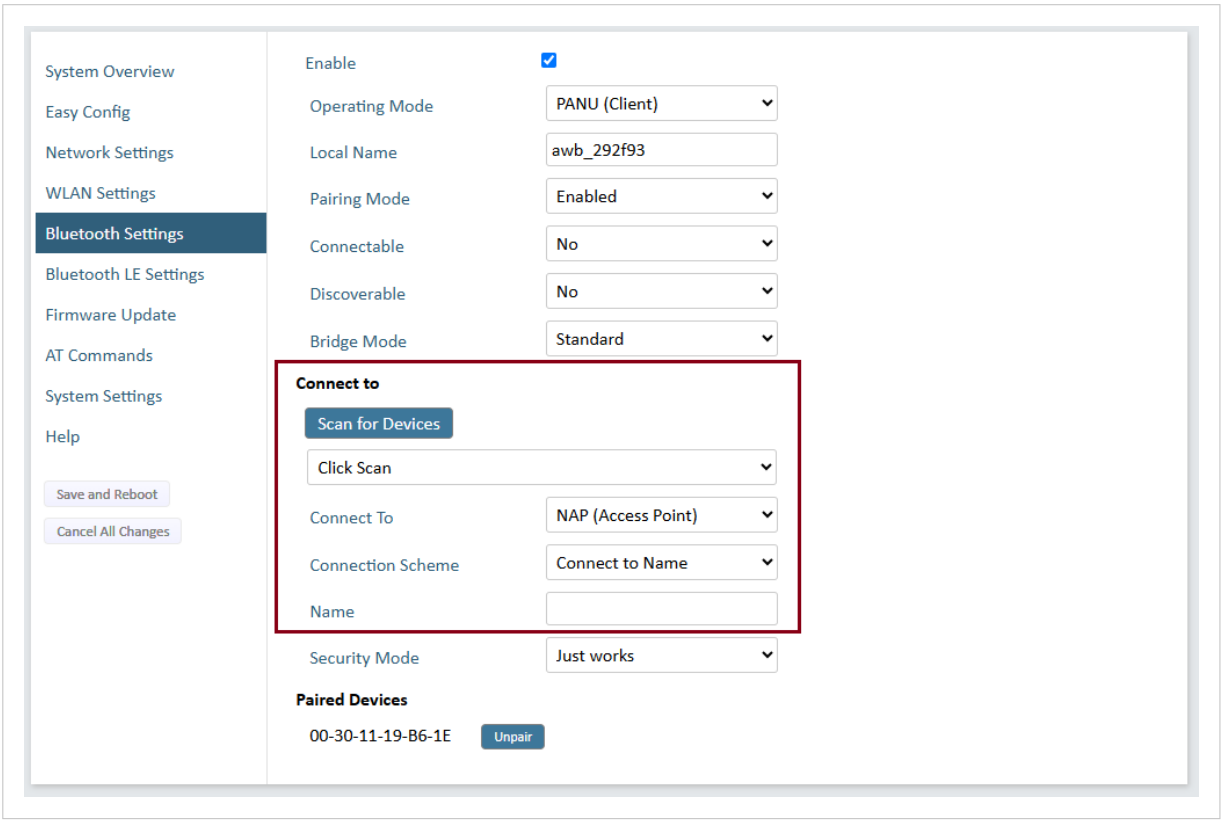


Figure 38. Bluetooth Settings page

Connect to settings for PANU Mode

Setting	Description
Scan for Devices	Scans the network for discoverable Bluetooth devices. To connect to a device, select it from the dropdown menu when the scan has completed.
Connect To	Used when connecting manually to a NAP or PANU device.
Connection Scheme	Choose whether to select a Bluetooth device by MAC address (default) or Name when connecting manually. Connecting to MAC will lock the connection to a specific hardware while connecting to Name allows for more flexibility.
MAC/Name	MAC address or Name of the Bluetooth device to connect to.

6.9.12. Bluetooth Settings for NAP Mode

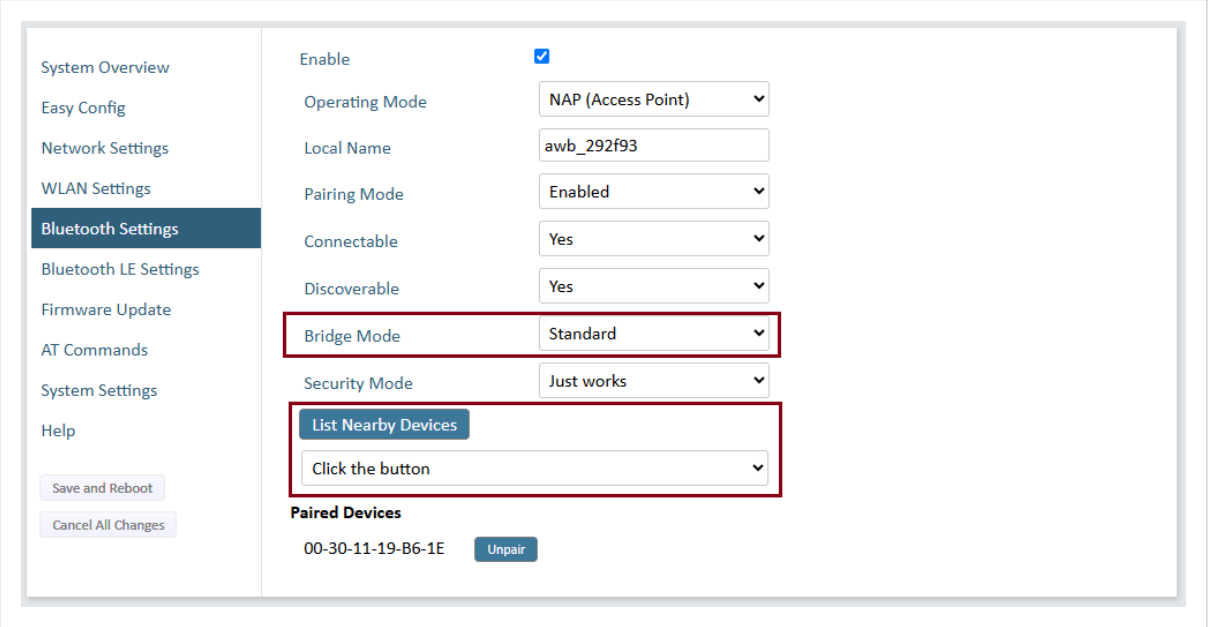


Figure 39. Bluetooth Settings page

Bluetooth Settings for NAP Mode

Setting	Description
Bridge Mode	**Standard** • Default mode. • Bridge data between devices without performing IP-level forwarding. **Layer 3 IP forward** • IP data is forwarded over Bluetooth. • Use when connecting to an Android device over Bluetooth. • Ensure the network has an active DHCP server to assign IP addresses.
List Nearby Devices	Scans the network and lists discoverable Bluetooth devices. Pairing cannot be initiated in NAP mode.

6.9.13. Bluetooth LE Settings

1. On the **Bluetooth Settings** page, enable **Bluetooth LE**.
2. On the **Bluetooth LE Settings** page, configure the Bluetooth LE settings.

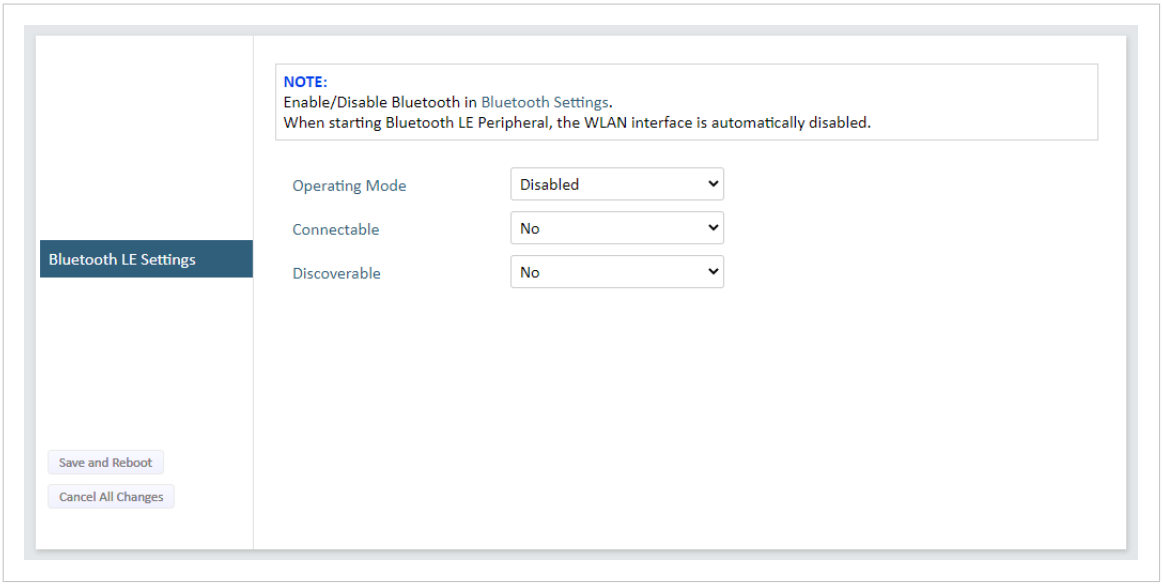


Figure 40. **Bluetooth LE Settings** page

Setting	Description
Operating Mode	**Disabled**: Bluetooth LE disabled (default) **Central**: Bluetooth LE Central operating mode enabled **Peripheral**: Bluetooth LE Peripheral operating mode enabled. This requires that the WLAN interface is disabled.
Connectable	**No**: Connectable is disabled (default) **Yes**: Enables the Wireless Bridge II Serial to search, connect and transfer data with another Bluetooth-capable device.
Discoverable	**No**: Discoverable is disabled (default) **Yes**: Enables the Wireless Bridge II Serial to pair with another Bluetooth-capable device.

6.9.14. System Settings

NOTE
Setting a secure password for the unit is strongly recommended.

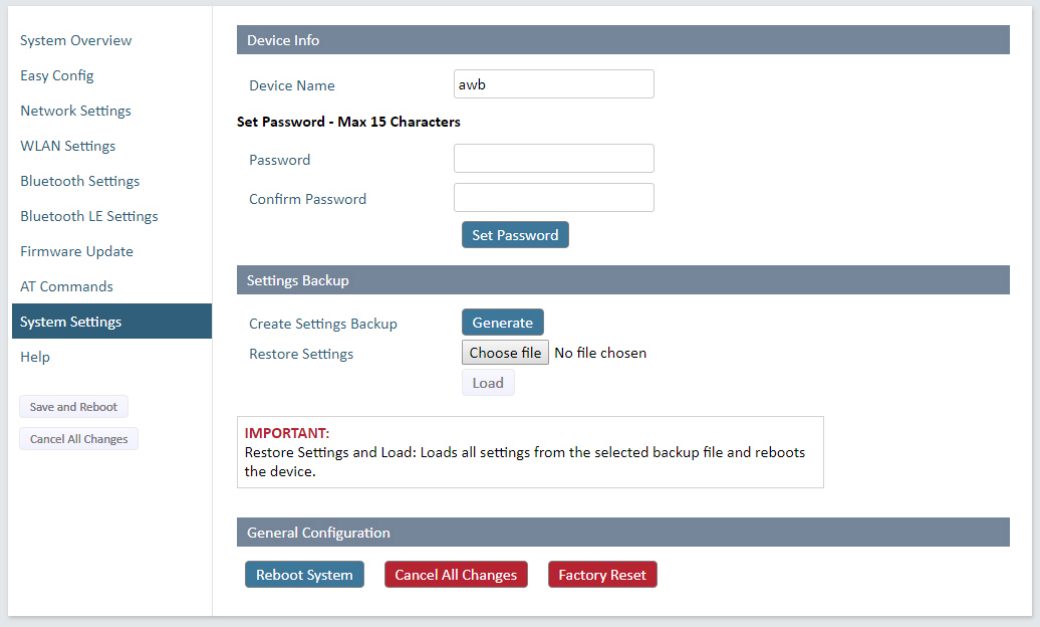


Figure 41. System Settings page

Device Info

Setting	Description
Device Name	Enter a descriptive name for the unit.
Password	Enter a password for accessing the web interface.

Local Configuration

IMPORTANT

You should only disable **Local configuration** if the Bridge II Ethernet is connected to trusted networks via routers or the wireless interface, and there are cybersecurity measures in place to protect the networks and connected devices from unauthorized access.

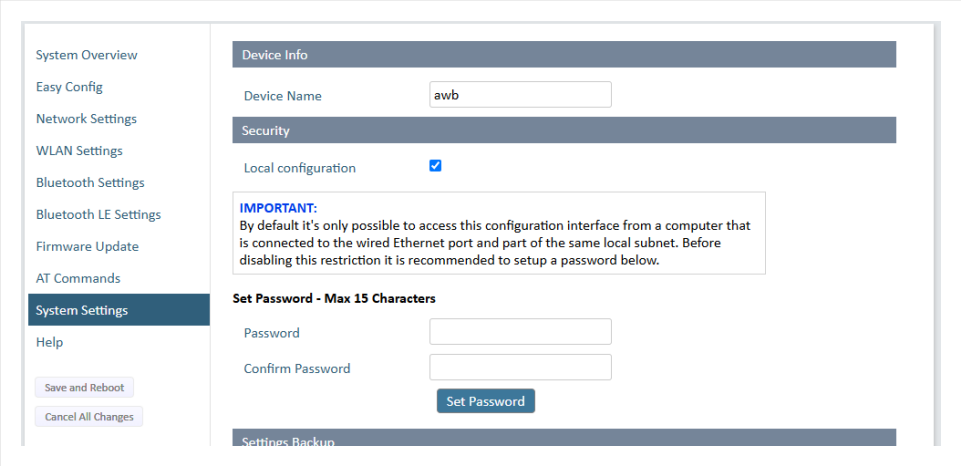


Figure 42. System Settings page, Security, Local configuration

By default, the **Local configuration** checkbox is selected, which restricts access to the Bridge II Ethernet built-in web interface.

This ensures only requests originating from the wired Ethernet interface and within the same sub network as the Bridge II Ethernet are permitted to access the built-in web interface.

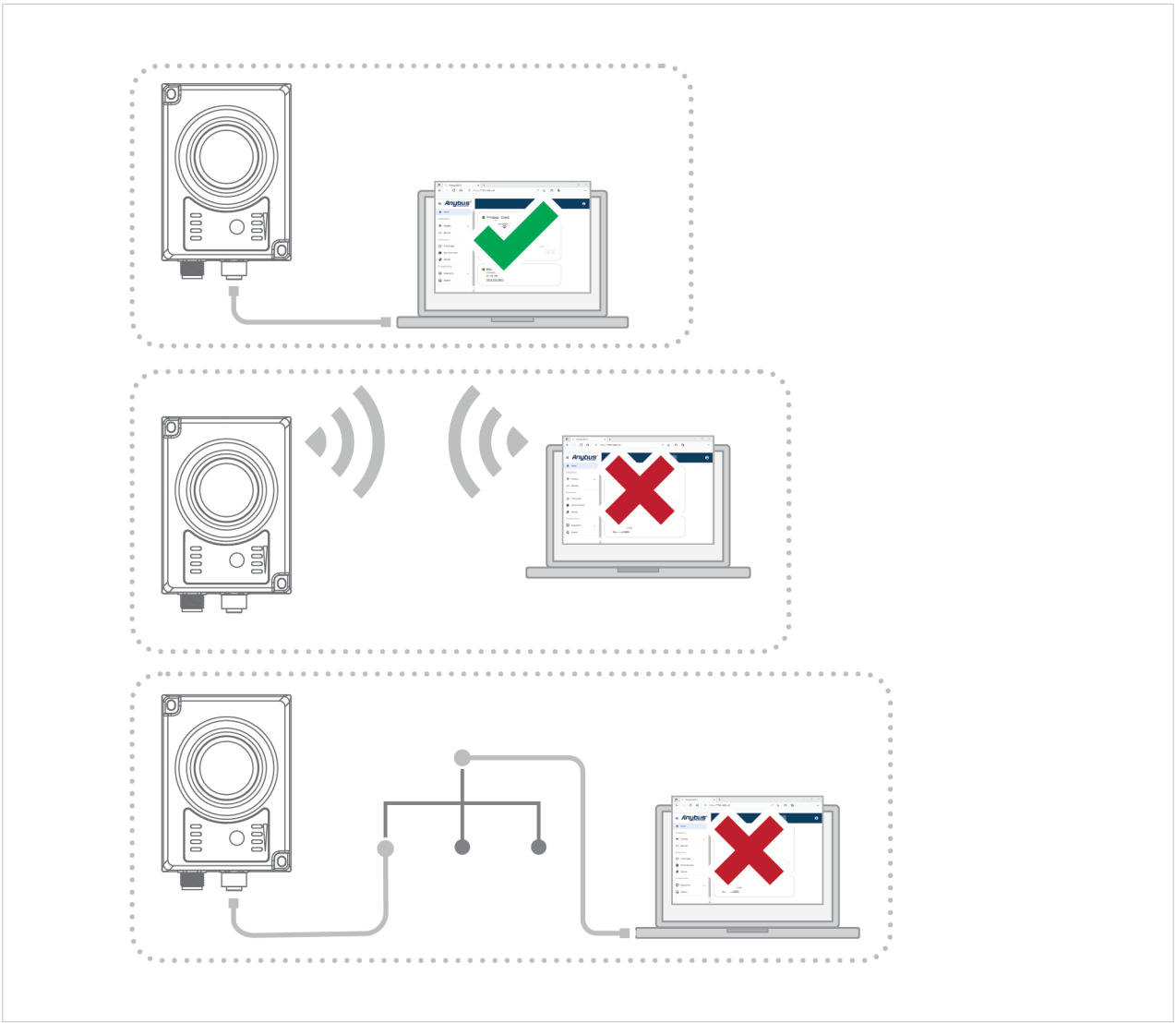


Figure 43. Direct LAN connection required for Bridge II Ethernet built-in web interface access

For a device to access the Bridge II Ethernet built-in web interface, connect it directly to the Bridge II Ethernet LAN (Local Area Network) port,

Settings Backup

Setting	Description
Create Settings Backup	Click Generate to save the current configuration to a file on your computer.
Restore Settings	Click Choose file and select a previously saved configuration, then click Load. The settings in the saved configuration will be applied and the unit will reboot.

General Configuration

Setting	Description
Reboot System	Reboots the system without applying changes.
Cancel All Changes	Restores all parameters in the web interface to the currently active values.
Factory Reset	Resets the unit to the factory default settings and reboots.

7. Verify Operation

7.1. LED Indicators

Status Indicators

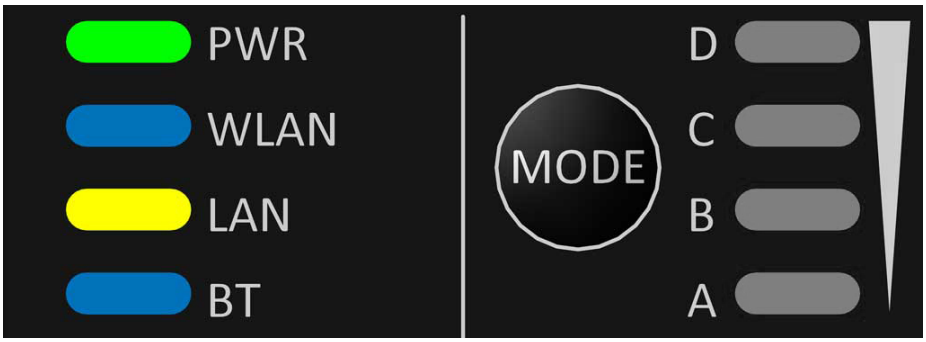


Figure 44. Status LED indicators

LED Indication		Description
PWR	Off	No power
	Green	Normal operation
WLAN	Off	WLAN disabled or no power
	Blue, blinking	Access Point: No clients, awaiting connections
	Blue	Access Point: Connected to at least one Client Client: Connected to Access Point
	Blue, flickering	WLAN data activity (when connected)
	Purple, blinking	Client: Scanning for access points
	Purple	Client: Connecting to a detected Access Point
	Red	Unrecoverable error
LAN	Off	No Ethernet connection
	Yellow	Ethernet link present
	Yellow, flickering	Ethernet data activity (when connected)
BT	Off	Bluetooth disabled or no power
	Blue, blinking	NAP: No clients, awaiting connections
	Blue	NAP: Connected to at least one PANU Client PANU: Connected to NAP
	Blue, flickering	Bluetooth data activity (when connected)
	Purple	PANU: Trying to connect to NAP
	Red	Unrecoverable error

Link Quality/Mode Indicators

The Link Quality/Mode Indicators are used to indicate Bluetooth quality, selected Easy Config mode and update status in Recovery Mode.

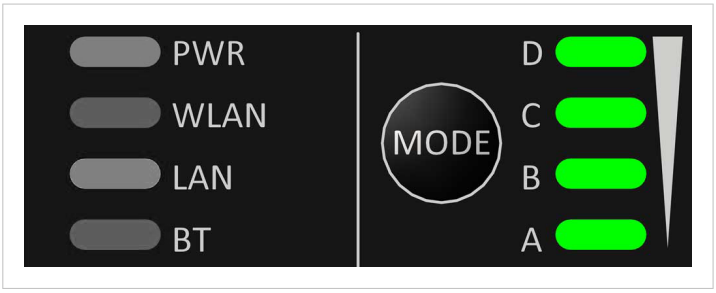


Figure 45. Link Quality/Mode indicators

Table 4. RSSI (WLAN Client) / Link Quality (Bluetooth PANU)

LED				Description
LED is off	LED is off	LED is off	LED is off	No connection
A, Green	LED is off	LED is off	LED is off	RSSI/Link Quality < 25 %
A, Green	**B**, Green	LED is off	LED is off	RSSI/Link Quality 25–50 %
A, Green	**B**, Green	**C**, Green	LED is off	RSSI/Link Quality 50–75 %
A, Green	**B**, Green	**C**, Green	**D**, Green	RSSI/Link Quality > 75 %

Recovery Mode LED Indications

Table 5. In Recovery Mode the Status LEDs indicate the firmware update status

LED	Indication	Description
PWR	Green	Firmware update in progress
	Green, blinking	Waiting for valid firmware
WLAN + **BT**	Alternating red/blue	Firmware update in progress

7.2. Network Connection Status

The **System Overview** page shows current settings and network connection status.

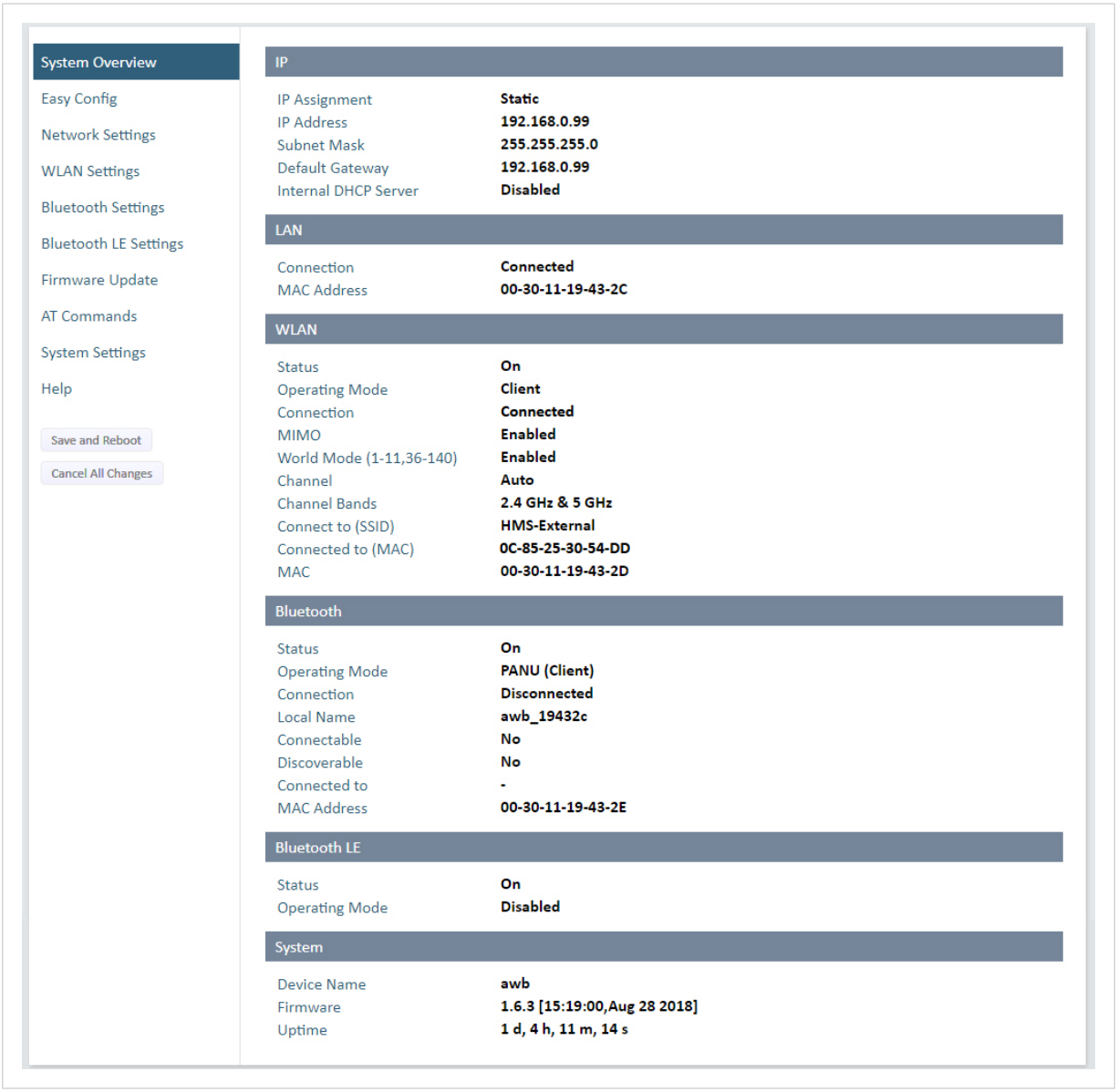


Figure 46. System Overview page example

8. Use Cases

8.1. Easy Config Using MODE Button: Confirm Connection Example

In this example, two Bridge II Ethernet units are configured with Easy Config using the **MODE** button.

For cybersecurity reasons, there is a mandatory step to confirm the connection between the two units to ensure that the correct devices are linked.

Procedure

1. When the Easy Config setup is started, Unit 1 becomes discoverable, and Unit 2 starts to search for Unit 1.
2. The Link Status LED indicators on each unit first blink to indicate that Easy Config mode is running.
3. When Unit 1 has discovered Unit 2, the Link Status LED indicators on both units start to blink a 5x4 LED pattern in a loop.
4. The LED blinking on the units are compared to ensure the blinking pattern match.

Example 6. LED indicators blinking patterns match

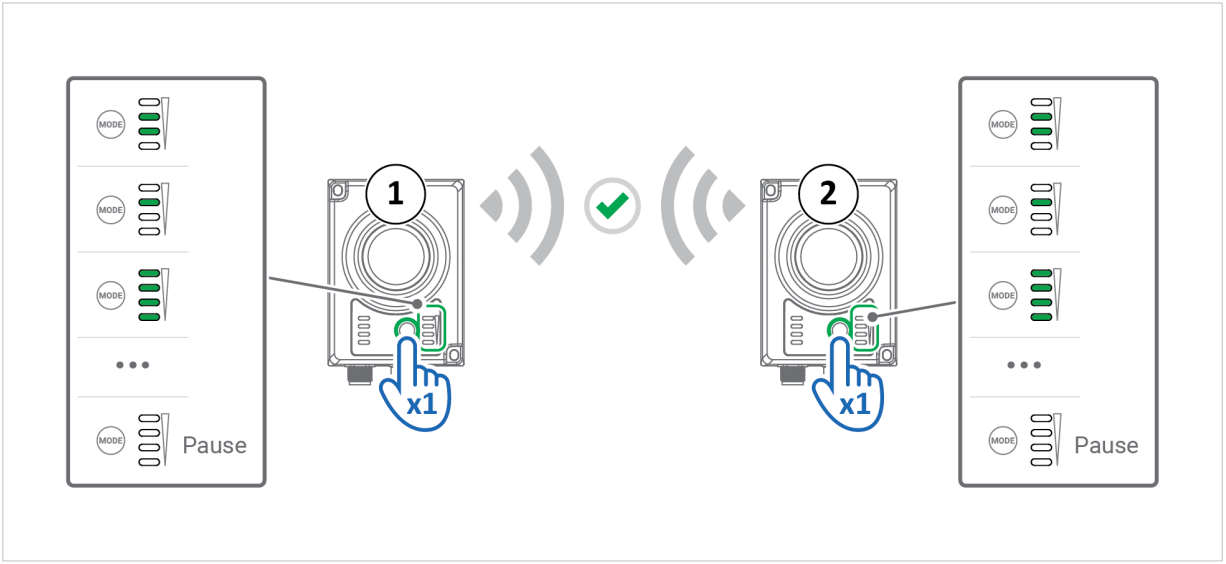


Figure 47. Codes match, Accept

The LED blinking pattern match on both Unit 1 and Unit 2.

To allow Unit 2 to connect to Unit 1, press the **MODE** button once on each unit.

Example 7. LED indicators blink on one unit only

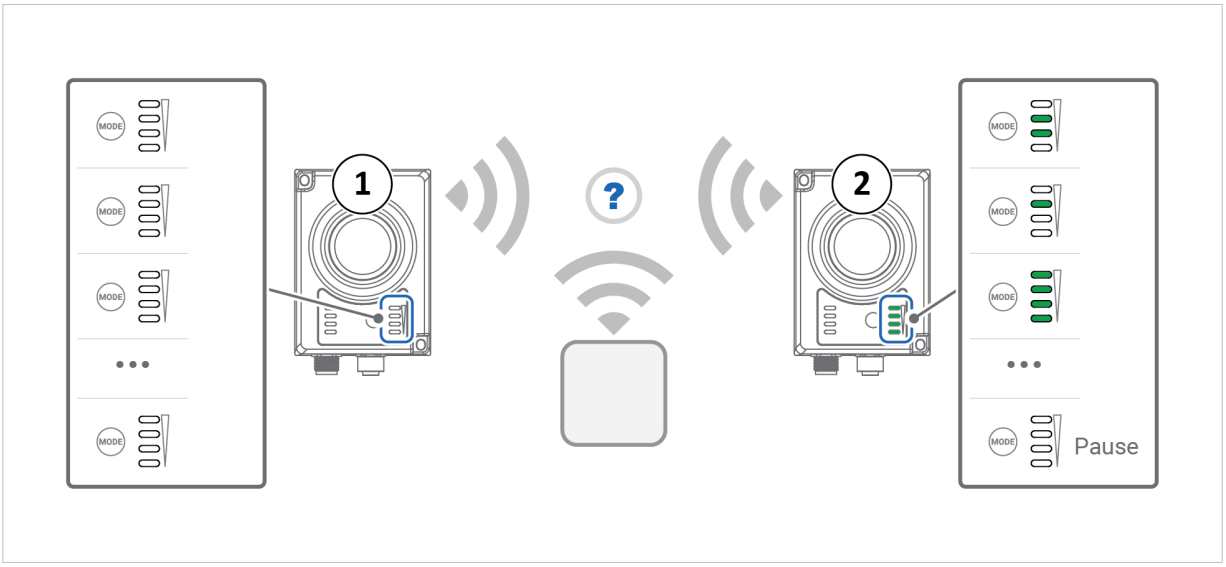


Figure 48. LED indicators blink on one unit only, wait for the Easy Config mode to timeout

Unit 2 has detected a device other than the Bridge II Ethernet Unit 1.

Wait for the Easy Config mode to time out; do not press the **MODE** button during this process.

Ensure that no other nearby Bluetooth devices are in pairing mode, then redo the Easy Config procedure.

Example 8. LED indicators blinking patterns do not match

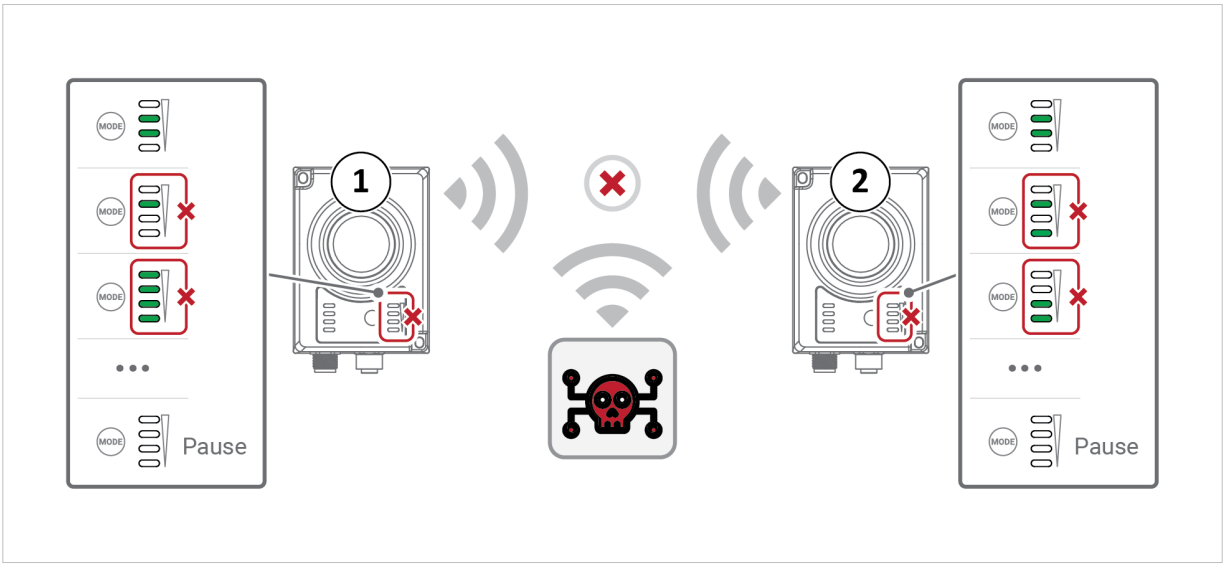


Figure 49. LED indicators blinking patterns do not match, wait for the Easy Config mode to timeout

The LED indicators blinking patterns do not match on both units; the code sequences are different.

This could indicate an attempt to intercept the bridged traffic via a third device.

Wait for the Easy Config mode to time out; do not press the **MODE** button during this process.

Verify that there are no unauthorized or potentially harmful devices in the area, then redo the Easy Config procedure.

8.2. Ethernet Bridge via WLAN or Bluetooth

Configuration with Easy Config

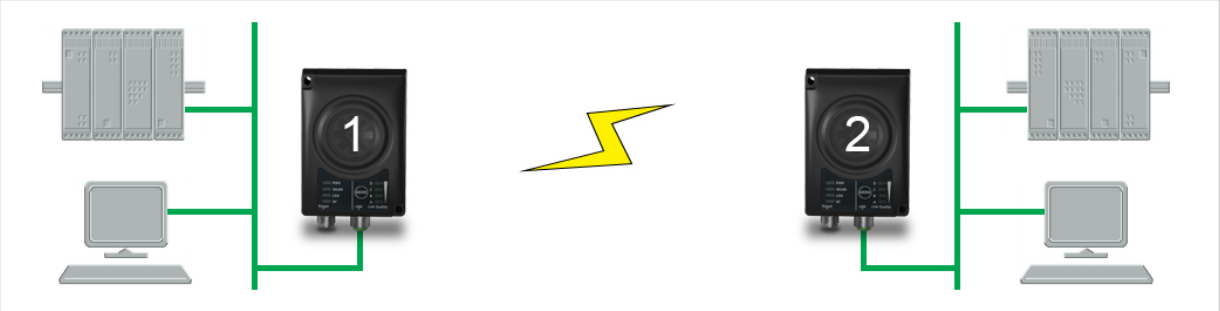


Figure 50. Ethernet bridge

This example describes how to connect two Ethernet network segments via WLAN or Bluetooth using Easy Config.

Set Up Unit 1

1. Power on Unit 1.
2. Wait for the LED indicators to light up and go out, then press **MODE** and release it immediately.
3. Press **MODE** repeatedly until LED C (Easy Config Mode 4) is lit.
4. To confirm, press and hold **MODE** for 2 seconds.
   Unit 1 is now discoverable.

Set Up Unit 2

1. Power on Unit 2.
2. Wait for the LED indicators to light up and go out, then press **MODE** and release it immediately.
3. Press **MODE** repeatedly until LED A and LED C (Easy Config Mode 5 - WLAN) or LED B and LED C (Easy Config Mode 5 Bluetooth) are lit.
4. To confirm, press and hold **MODE** for 2 seconds.

Confirm Connection

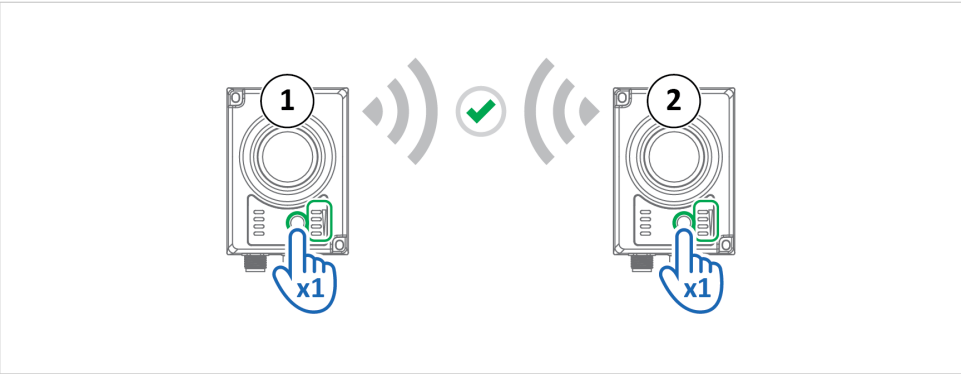


Figure 51. Codes match, Accept

For cybersecurity reasons, the following steps are implemented to ensure the correct devices are connected:

1. The Link Status LED indicators on each unit first blink to indicate that Easy Config mode is running.
2. When Unit 1 has discovered Unit 2, the Link Status LED indicators on both units start to blink a 5x4 LED pattern in a loop.

3. Compare the units to ensure that the LED indicators flash in the same pattern.
   - To allow Unit 2 to connect to Unit 1, press the **MODE** button once on each unit.
   - If Unit 2 detects a device other than the Bridge II Ethernet Unit 1, wait for the Easy Config mode to time out.
     Do not press the **MODE** button during this process.
     Ensure that no other nearby Bluetooth devices are in pairing mode, then redo the Easy Config procedure.
   - If the LED indicators blinking patterns do not match on both units, wait for the Easy Config mode to time out.
     Do not press the **MODE** buttons during this process.
     Verify that there are no unauthorized or potentially harmful devices in the area, then redo the Easy Config procedure.

Result

- Unit 1 is now open for automatic configuration.
- Unit 2 will discover and configure Unit 1 as a Client and configure itself as an Access Point.
- Unit 1 will be assigned the first free IP address in the same Ethernet subnet as Unit 2.

Add Additional Units

To add a Client Unit, repeat the configuration steps.

- You can add up to 6 additional Clients, by repeating the procedure.
- Each new Client will be assigned the next free IP address in the current subnet.

8.3. PROFINET Networking Via Bluetooth

Configuration with Easy Config

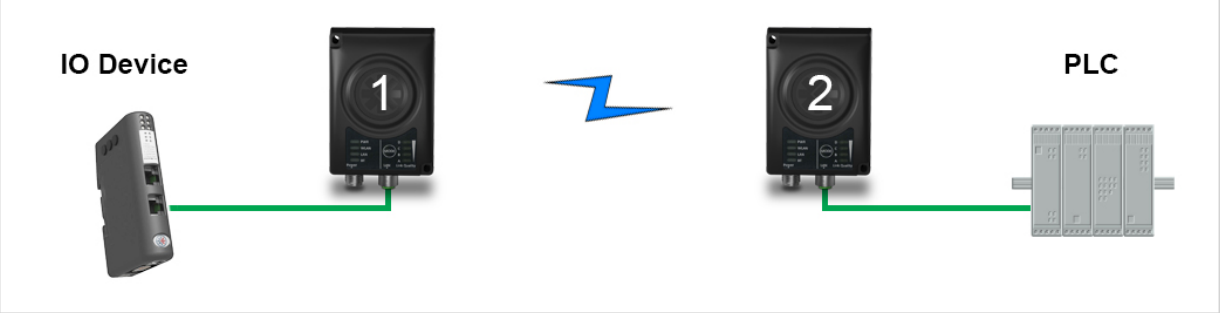


Figure 52. PROFINET wireless network

This example describes how to connect a PROFINET IO device and a PROFINET PLC over Bluetooth using two Bridge II Ethernets and Easy Config.

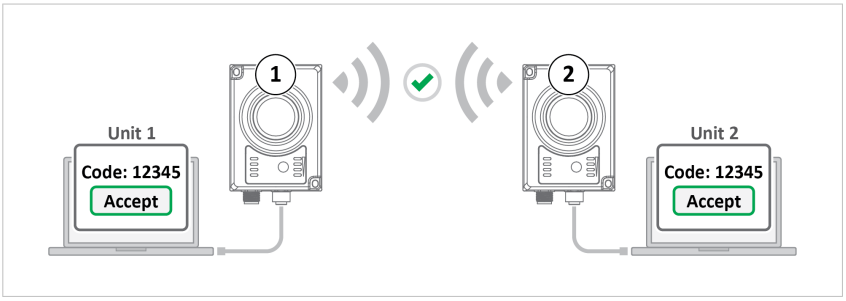
The Bridge II Ethernets are configured with PROFINET optimization. This means that PROFINET messages have priority over TCP/IP frames.

See the respective documentation for the IO device and PLC on how to configure them for PROFINET communication.

Activate Easy Config Mode

1. Reset both units to the factory default settings.
2. Connect Unit 1 to the IO device and Unit 2 to the PLC.
3. Set Unit 1 to Easy Config Mode 4.
   Unit 1 is now discoverable.
4. Set Unit 2 to Easy Config Mode 8.

Confirm Connection



For cybersecurity reasons, the following steps are implemented to ensure the correct devices are connected:

1. On the **Easy Config** page for each unit, a dialog window appears showing an **Easy Config confirmation** code.

2. Compare the codes displayed in the dialog windows of both units to ensure they are identical.
   - To allow Unit 2 to connect to and configure Unit 1, click **Accept** for each unit,
   - If Unit 2 cannot discover Unit 1, the dialog window only appear on Unit 2. Then, click **Reject**.
     Ensure that no other nearby Bluetooth devices are in pairing mode, then redo the Easy Config procedure.
   - If the codes do not match, click **Reject**.
     Verify that there are no unauthorized or potentially harmful devices in the area, then redo the Easy Config procedure.

Result

- Unit 1 is now open for automatic configuration.
- Unit 2 will now automatically discover and configure Unit 1 as a Bluetooth Client, and configure itself as an Access Point.
- Both units are optimized for PROFINET.
- The IO device will now be able to communicate with the PLC as if using a wired connection.

Add Additional Units

NOTE
The IO cycle update time for each IO device must be set to ≥ 64 ms.

To add a Client Unit, repeat the configuration steps.

- You can add up to 6 additional Clients, by repeating the procedure.
- Each new Client will be assigned the next free IP address in the current subnet.

8.4. EtherNet/IP Networking Via Bluetooth

Configuration with Easy Config

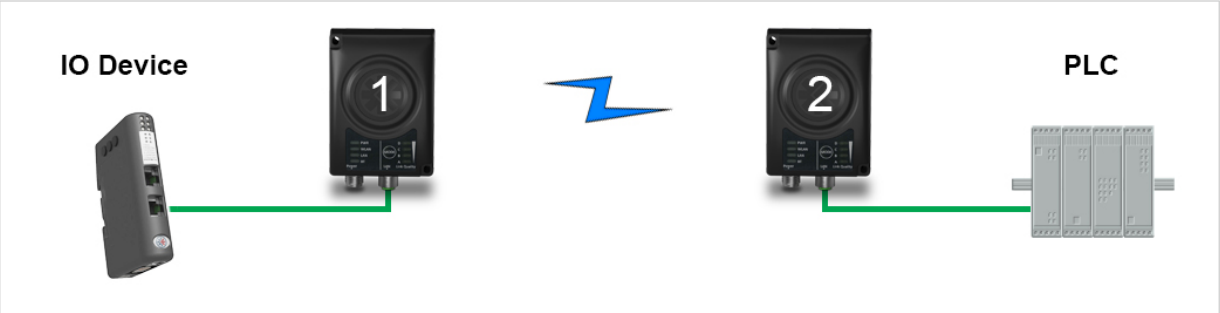


Figure 53. EtherNet/IP wireless network

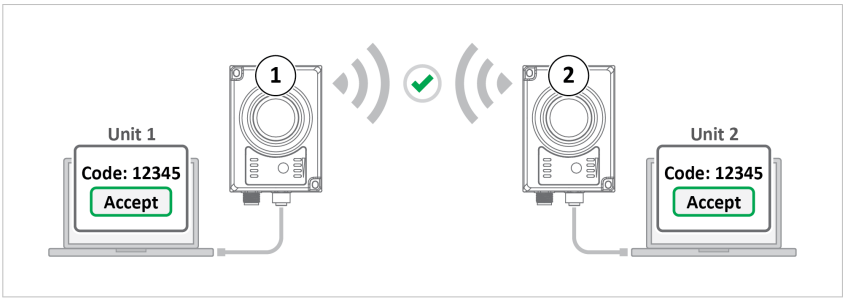
This example describes how to connect an EtherNet/IP IO device and an EtherNet/IP PLC over Bluetooth using two Wireless Bridges and Easy Config.

See the respective documentation for the IO device and PLC on how to configure them for EtherNet/IP communication.

Activate Easy Config Mode

1. Reset both units to the factory default settings.
2. Connect Unit 1 to the IO device.
3. Connect Unit 2 to the PLC.
4. Set Unit 1 to Easy Config Mode 4.
   Unit 1 is now be discoverable.
5. Set Unit 2 to Easy Config Mode 6

Confirm Connection



For cybersecurity reasons, the following steps are implemented to ensure the correct devices are connected:

1. On the **Easy Config** page for each unit, a dialog window appears showing an **Easy Config confirmation** code.
2. Compare the codes displayed in the dialog windows of both units to ensure they are identical.
   - To allow Unit 2 to connect to and configure Unit 1, click **Accept** for each unit,
   - If Unit 2 cannot discover Unit 1, the dialog window only appear on Unit 2. Then, click **Reject**.
     Ensure that no other nearby Bluetooth devices are in pairing mode, then redo the Easy Config procedure.
   - If the codes do not match, click **Reject**.
     Verify that there are no unauthorized or potentially harmful devices in the area, then redo the Easy Config procedure.

Result

- Unit 1 is now open for automatic configuration.
- Unit 2 will automatically discover and configure Unit 1 as a Bluetooth Client, and configure itself as an Access Point.
- The IO device will now be able to communicate with the PLC as if using a wired connection.

Add Additional Units

NOTE
The Requested Packet Interval (RPI) for each IO device must be set to ≥ 64 ms.

To add a Client Unit, repeat the configuration steps.

- You can add up to 6 additional Clients, by repeating the procedure.
- Each new Client will be assigned the next free IP address in the current subnet.

8.5. Ethernet Network to Existing WLAN

Figure 54. Connecting to a WLAN

This example describes how to connect a machine with an internal Ethernet network to an existing WLAN.

This setup allows traffic on network layer 3, but not layer 2. This means that TCP/IP based protocols such as EtherNet/IP, Modbus TCP and BACnet can be used on the WLAN, but not protocols that use layer 2 traffic, such as PROFINET.

Before You Begin

- When using this set up in an enterprise network, read the connectivity consideration information before you start. Layer 3 IP Forward Connectivity Considerations (page 38).

Configuration

1. Reset the Bridge II Ethernet to the factory default settings.
2. In **Network Settings**, configure the IP settings as required by the wireless network.
3. If the network uses DHCP, select **DHCP Relay Enabled**.

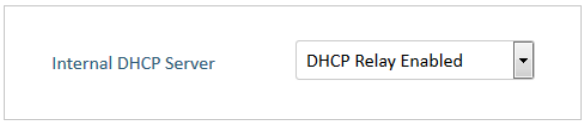


Figure 55. DHCP Relay Enabled

WLAN Settings for Small Office/Home Office Network

When the setup is used in a small office/home office network, follow these steps:

1. In **WLAN Settings**, select **Layer 3 IP forward** (default setting) from the **Bridge Mode** drop-down list.
2. In **WLAN Settings**, click **Scan for Networks**.
3. When the scan is completed, select the wireless network from the drop-down list.
4. If required, select the authentication mode and enter the passkey for the wireless network.
5. Click **Save and Reboot**.
   The Ethernet network will now be able to access the WLAN Access Point.

WLAN Settings for Enterprise Network

When the setup is used in an enterprise network, follow these steps:

1. In WLAN Settings, set **Bridge Mode** to **Layer 2 cloned MAC only**.

2. In the **Cloned MAC Address** field, enter the MAC address of the PLC.
3. In the **Cloned IP Address** field, enter the IP address of the PLC.
4. Click **Save and Reboot**.
   The Bridge II Ethernet will now function as a WLAN interface for the PLC using the MAC address of its Ethernet interface.

8.6. Adding Single Ethernet Node to WLAN

Figure 56. Adding WLAN connectivity

This example describehows how to connect a PLC with an Ethernet network interface to an existing WLAN with support for layer 2 and layer 3 traffic. The WLAN interface in the Bridge II Ethernet will clone the MAC address of the Ethernet interface in the PLC.

Only a single Ethernet node will be able to communicate via a third-party WLAN Access Point in this setup.

Configuration

1. Reset the Bridge II Ethernet to the factory default settings.
2. In **Network Settings**, configure the IP settings as required by the wireless network.
3. In WLAN Settings, click on **Scan for Networks**.
4. When the scan is completed, select the wireless network from the drop-down list.
5. If required, select the authentication mode and enter the passkey for the wireless network.
6. Click **Save and Reboot**.
7. To ensure that the WLAN connection is established, check the **System Overview** page.

> **NOTE**
> It is important that the WLAN connection is established before you proceed with the next configuration step. When the final configuration step is done, the built-in web interface may no longer be accessible from the network without performing a factory reset.

8. In **WLAN Settings**, set **Bridge Mode** to **Layer 2 cloned MAC only**.
9. In the **Cloned MAC Address** field, enter the PLC MAC address.
10. In the **Cloned IP Address** field, enter the PLC IP address.
11. Click **Save and Reboot**.
    The Bridge II Ethernet will now function as a WLAN interface for the PLC using the MAC address of its Ethernet interface.

8.7. Access PLC from Handheld Device via WLAN

Figure 57. Access a PLC from a handheld device using WLAN

This example describes how to use a Bridge II Ethernet to access the web interface of a PLC on a wired network from a tablet or smartphone which uses DHCP. The Bridge II Ethernet will function as a WLAN Access Point.

Before You Begin

- Please refer to the documentation for the handheld device and PLC on how to configure their respective network settings.

Configuration

1. Reset the Bridge II Ethernet to the factory default settings.
2. In **Network Settings**, configure the IP settings as required:

Option if the wired network uses DHCP

a. Select **DHCP Relay Enabled**.

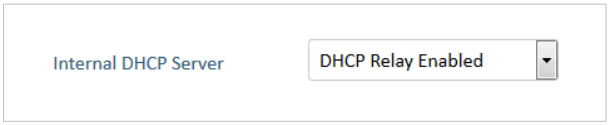


Figure 58. DHCP Relay Enabled

Option if the wired network uses static IP

> **IMPORTANT**
> To avoid IP address conflict if a DHCP server is already active on the network, use the DHCP Interfaces setting to limit the internal DHCP server to the correct interface.

a. Select **DHCP Server Enabled**.
b. Select an interface from the **DHCP Interfaces** drop-down menu.

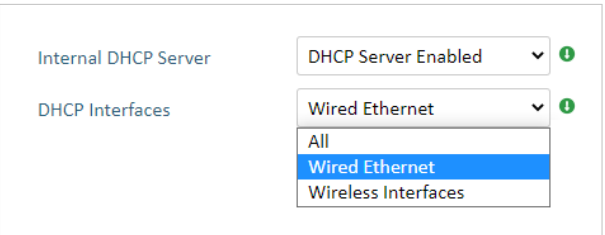


Figure 59. DHCP Interfaces, Wired Ethernet

c. Enter a Start Address for DHCP addressing. Ensure that the address range does not contain any existing addresses on the network.

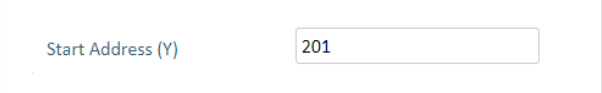


Figure 60. Start Address for DHCP addressing

The Bridge II Ethernet will now function as a DHCP server and allocate an IP address to the handheld device over WLAN.

3. In **WLAN Settings**, set **Operating Mode** to **Access Point**.

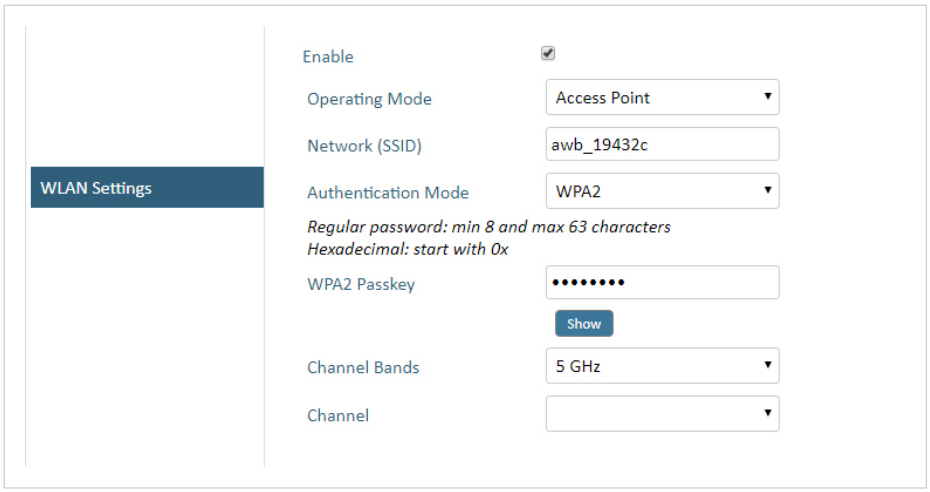


Figure 61. WLAN Settings

4. Enter a unique **Network (SSID)**, network name, for the new wireless network.
5. Set **Authentication Mode** to **WPA2** and enter a passkey.
6. Select a **Channel band** and a **Channel**.
7. Click **Save and Reboot**.
   You should now be able to connect to the SSID of the Bridge II Ethernet on your handheld device and access the PLC by by entering its IP address in a browser.

9. Maintenance

9.1. Manually Update Firmware

Before You Begin

NOTE
For manual firmware installation to work, make sure **Automatic Update Mode** is **Disabled**.

NOTE
The configuration settings are not affected when updating firmware.

Download the Firmware Update File

1. Download the firmware update file from www.hms-networks.com/technical-support.
2. Connect Bridge II Ethernet to your computer, refer to Connect to Configure (page 16).

Procedure

Update the Bridge II Ethernet firmware.

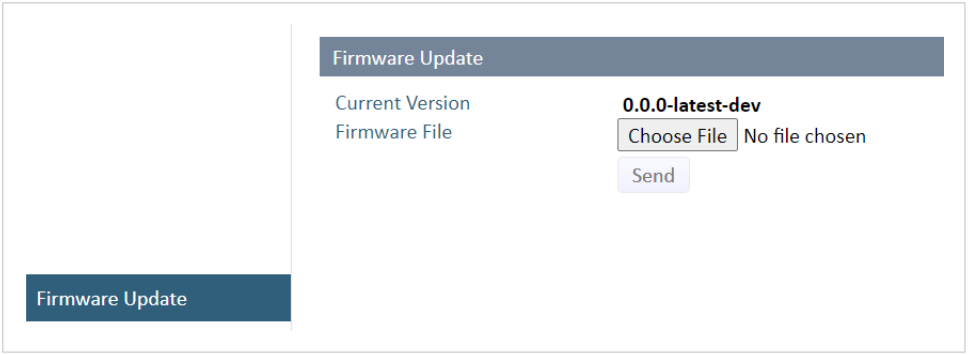


Figure 62. Firmware Update, Choose file

1. Click **Choose File**.
2. In the **Open** dialog box, browse to and select the firmware update file and click **Open**.
3. To start the file transfer, click **Send**.

NOTE
Do not refresh or leave the Firmware Update page until the process has finished.

Firmware update progress

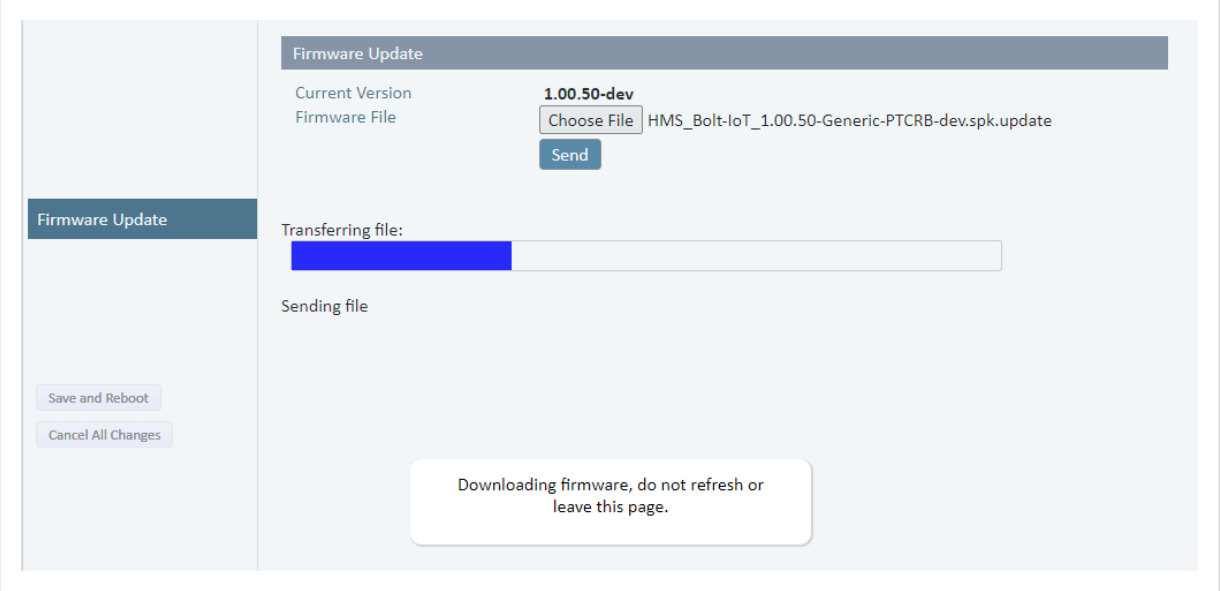


Figure 63. Firmware Update, Transferring file

- The progress bar, Transferring file, indicates the progress of the file transfer. Status messages show the progress of the firmware update stages.
- When the file transfer is finished, the progress bar turns green.

Reboot

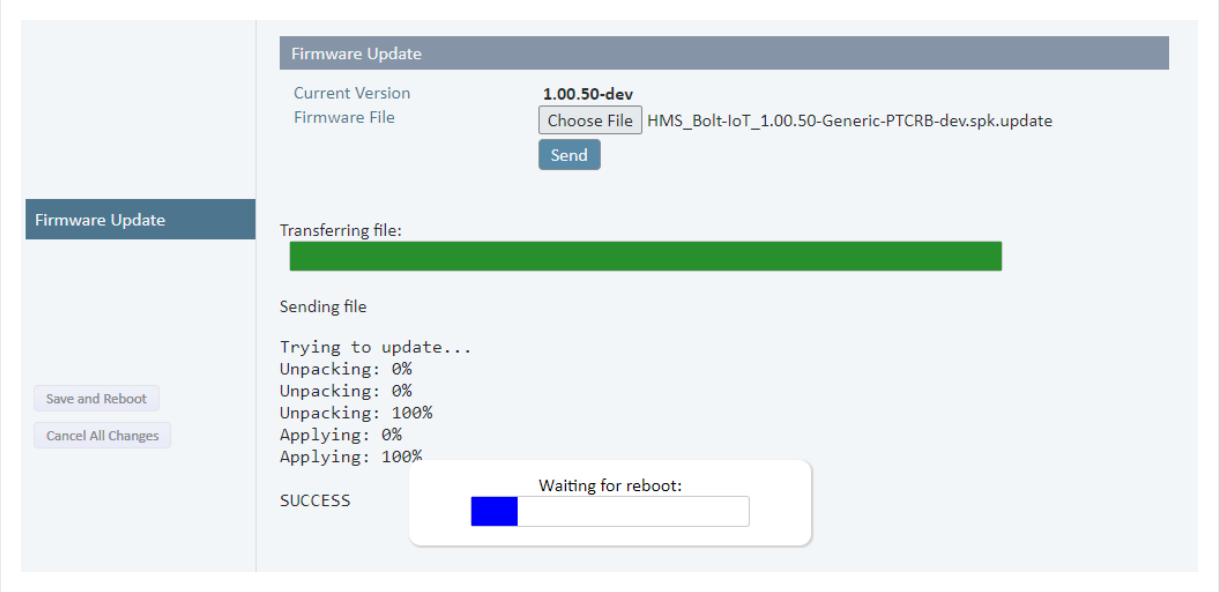


Figure 64. Firmware Update, Waiting for reboot

- When the firmware update is finished, Bridge II Ethernet automatically reboots for the updates to take effect. The progress bar, Waiting for reboot, indicates the progress.
- When the reboot is complete, the web browser automatically redirects to the **System Overview** page.

9.2. Automatically Check for Firmware Updates

By default **Automatic Update Mode** is **Disabled**.

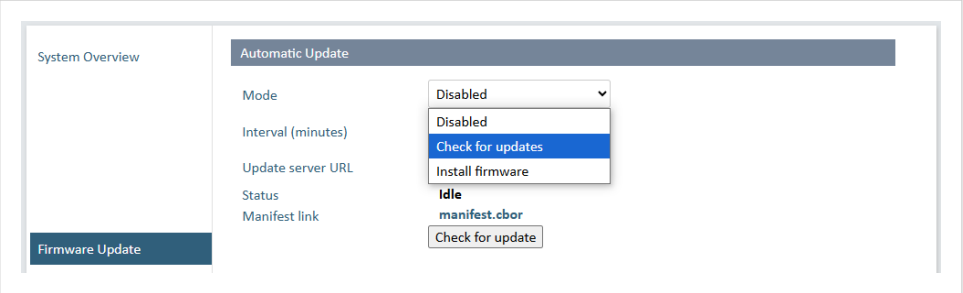


Figure 65. Automatic Update Mode menu, Check for updates

Check for Updates Settings

1. From the **Mode** menu, select **Check for Updates**.
2. In the **Interval** field, specify the frequency in minutes (0-10 000) at which the Bridge II Ethernet should check for new firmware updates.
   The Bridge II Ethernet checks for updates at each boot, and then periodically at the configured interval.
   For the Bridge II Ethernet to check for updates only at boot, set the interval to 0.
3. By default, the firmware is downloaded from a vendor-operated upgrade server.
   To use your own update server, enter its URL in the the **Manifest URL** field. The firmware will be downloaded automatically from this address.

Automated Firmware Search and Download

The Bridge II Ethernet will check for new firmware every [specified number] hour(s).

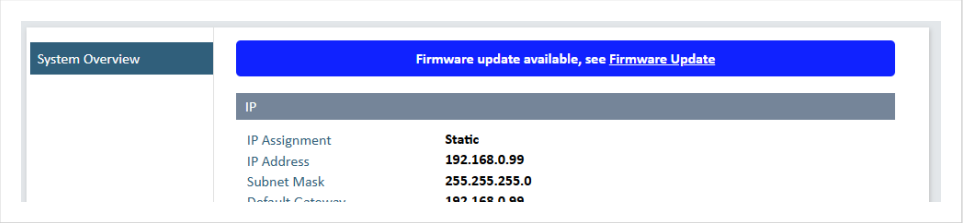


Figure 66. Firmware update available banner

If an firmware update is available, a banner appear below the header indicating that new firmware is ready for installation.

Firmware Installation

To install the firmware, click **Install firmware**.

The firmware is downloaded and installed.

When the firmware installation is completed, the progress bar turn green and the Bridge II Ethernet automatically reboots.

9.3. Automatically Update Firmware

By default **Automatic Update Mode** is **Disabled**.

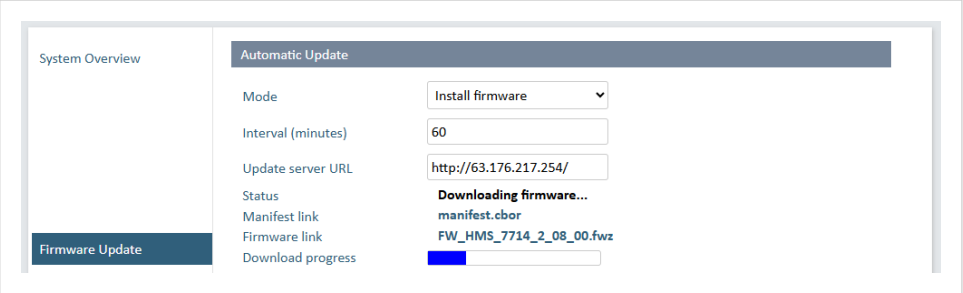


Figure 67. Automatic Update Mode menu, Install firmware

Procedure

1. From the **Mode** menu, select **Install firmware**.
2. In the **Interval** field, enter how often, in minutes, the Bridge II Ethernet should check for new firmware updates.
   For the Bridge II Ethernet to check for updates on each boot, enter 0.

Result

The Bridge II Ethernet will check for new firmware every [specified interval] hour(s).

If an update is available, it is automatically downloaded and installed.

The Bridge II Ethernet automatically reboots, for the upgrade to take effect.

9.4. Settings Backup

9.4.1. Create Settings Backup File

IMPORTANT
The Administrator Password is not saved in the settings backup file.

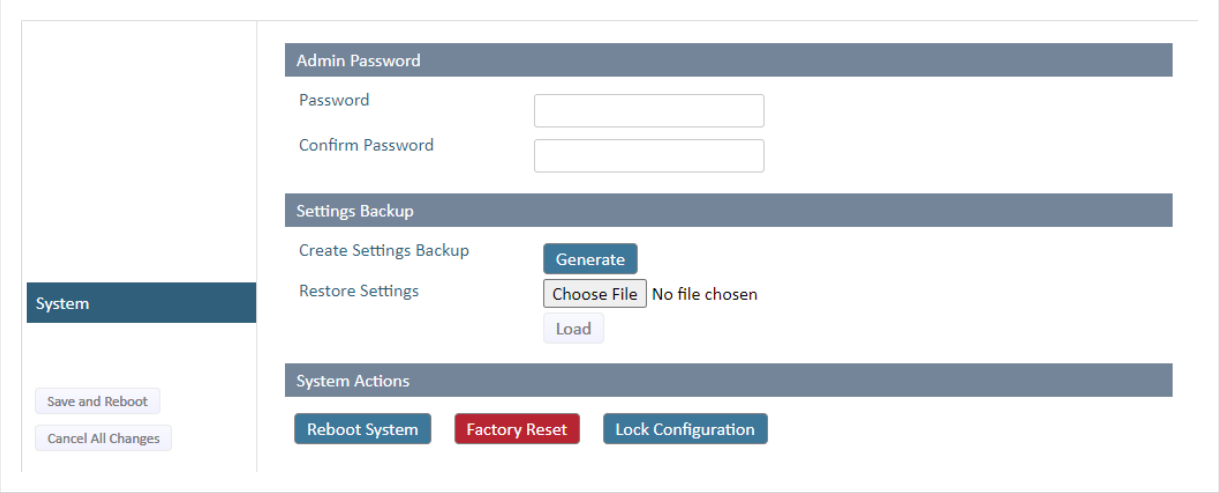


Figure 68. System page

To save the current configuration in a backup file, click **Generate**.

A backup file is automatically downloaded and saved in the Downloads folder on your PC.

9.4.2. Restore Settings From Backup File

IMPORTANT
When you restore settings from a backup file, all the current settings except the Administrator Password are overwritten by the settings loaded from the backup file.

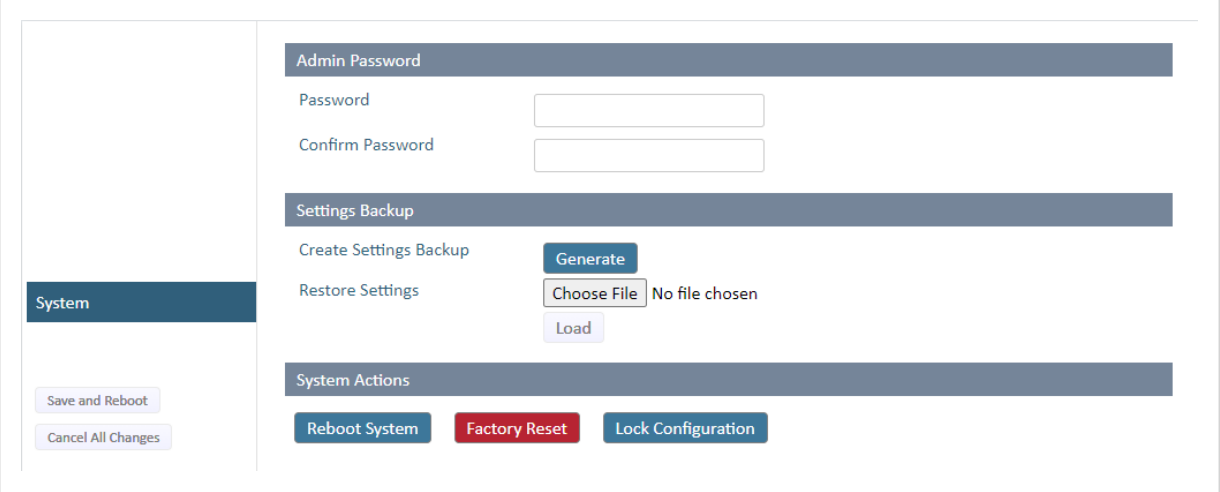


Figure 69. Restore Settings from a backup file

Restore settings from a backup file

1. Click **Choose** file.
2. Browse to and select your backup file.
3. Click **Load**.
   The Bridge II Ethernet reboot automatically, for the settings loaded from the backup file to take effect.

10. Troubleshooting

10.1. Recovery Mode

If the built-in web interface cannot be accessed, the unit can be reset by starting in Recovery Mode and reinstalling the firmware.

Before You Begin

IMPORTANT
Use Recovery Mode only when the unit is unresponsive and the built-in web interface cannot be accessed. Firmware updates should normally be carried out through the built-in web interface.

Procedure

To enter Recovery Mode

1. Press and hold **MODE** button during startup.

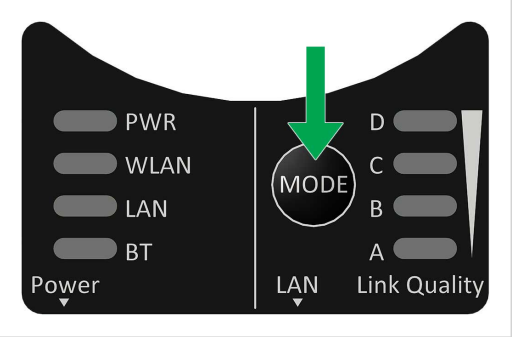


Figure 70. **MODE** button

2. Bridge II Ethernet enters Recovery Mode.

Table 6. In Recovery Mode the Status LEDs indicate the firmware update status

LED	Indication	Description
PWR	Green	Firmware update in progress
	Green, blinking	Waiting for valid firmware
WLAN + **BT**	Alternating red/blue	Firmware update in progress

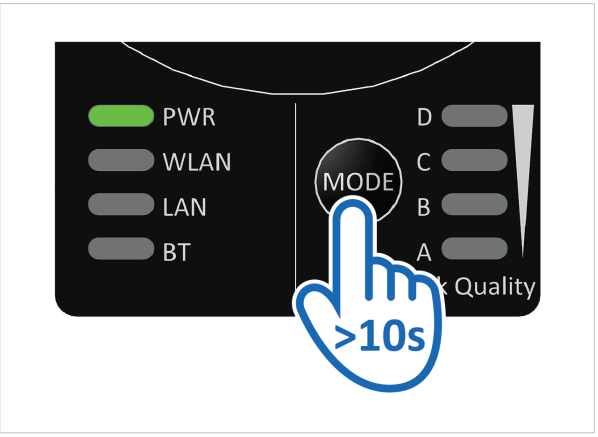
To Reinstall the Firmware

1. To reinstalling the firmware, you need Anybus Firmware Manager II.
   Download Anybus Firmware Manager II from www.hms-networks.com/technical-support.
2. Install Anybus Firmware Manager II on your PC.
3. Launch Anybus Firmware Manager II and follow the instructions to reinstall the firmware.

10.2. Reset to Factory Default

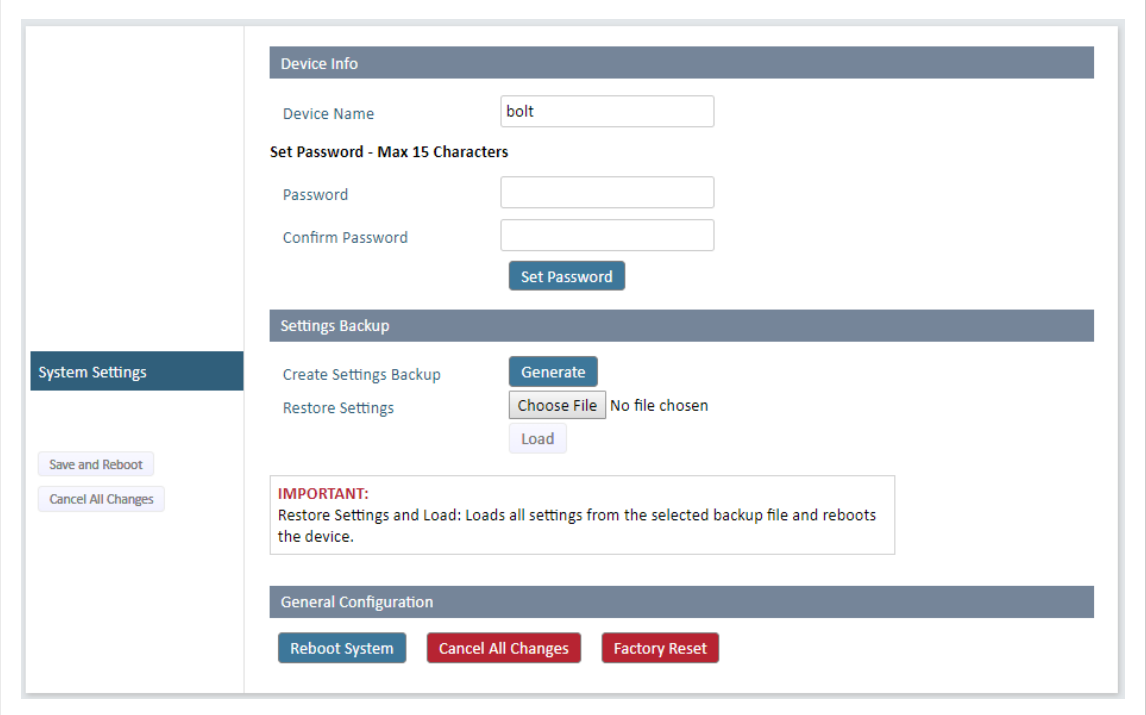
Any one of these actions will restore the unit to factory default settings.

Reset Using the MODE Button



To reset Bridge II Ethernet to factory default, press and hold **MODE** for >10 seconds and then release it.

Reset Via the Built-In Web Interface



Launch the built-in web interface > On the **System Settings** page, click **Factory Restore**.

Reset Using Easy Config

To reset Bridge II Ethernet to factory default, execute Easy Config Mode 2.

See Activate an Easy Config Mode in the Built-In Web Interface.

Reset Using AT Command

To reset Bridge II Ethernet to factory default, issue the AT command **AT&F** and then restart the unit.

See Configuration with AT Commands (page 31).

Reset Using Digital Input

To reset Bridge II Ethernet to factory default, apply voltage to the digital input for >10 seconds.

See Connect to LAN and Power (page 13).

11. End Product Life Cycle

11.1. Secure Data Disposal

IMPORTANT
To reduce the risk of sensitive data exposure, always perform a factory reset before decommissioning the equipment.

A factory reset will reset any on-site made configuration changes and revert the Bridge II Ethernet to the default settings of the latest installed firmware version.

See Reset to Factory Default (page 75).

12. Technical Data

12.1. Technical Specifications

Hardware Specifications

Order code	AWB3000	AWB3010
Wired Interface type	Ethernet	
Antenna	3 internal antennas: 2.4 GHz 2.4 GHz MIMO 5 GHz	1 external antenna: 2.4 GHz + 5 GHz dual band
	The external antenna does not provide better range but allows connectivity if the Wireless Bridge needs to be placed inside a radio-secure environment such as a steel cabinet. When mounting inside a steel cabinet antenna cables with magnetic foot or screw mount should also be considered.	
Dimensions (LxWxH)	93 x 68 x 33.2 mm	
Weight	120 g	
Operating temperature	-40 to +65 °C	
Storage temperature	-40 to +85 °C	
Humidity	EN 600068-2-78: Damp heat, +40 °C, 93 % humidity for 4 days	
Vibration	See datasheet	
Housing material	Plastic (see datasheet for details)	
Protection class	Class III (SELV)	
IP rating	IP65	
Mounting	Screw mount or DIN rail using optional clip	
Power connector	M12 male A-coded	
Ethernet connector	M12 female D-coded	
Power supply	9–30 VDC (-5 % +20 %) Cranking 12 V (ISO 7637-2:2011 pulse 4) Reverse polarity protection	
Power consumption	0.7 W (idle), 1.7 W (max)	

Communication

Ethernet	
Ethernet interface	10/100BASE-T with automatic MDI/MDIX auto cross-over detection
Ethernet protocols	IP, TCP, UDP, HTTP, LLDP, ARP, DHCP Client/Server, DNS support Transparent transfer of PROFINET IO, EtherNet/IP, Modbus-TCP or any other TCP/UDP based protocol

Wireless LAN	
Wireless standards	IEEE 802.11 a, b, g, n, d, r
Operation modes	Access point or Client
Fast roaming	IEEE 802.11r (Client)
Max. number of clients for Access Point	7
WLAN channels	2.4 GHz Access Point: 1–11 2.4 GHz Client: 1–11 + 12 & 13 depending on regulatory domain scan 5 GHz Access Point: 36–48 (U-NII-1) 5 GHz Client: 36-48 + 100–116, 132–140, 120–128 depending on regulatory domain scan. (U- NII-1, U-NII-2, U-NII-2e)
RF output power	18 dBm EIRP (including max antenna gain 3 dBi)

Wireless LAN	
Power consumption	54 mA @ 24 VDC
Net data throughput	20 Mbps.
Link speed	Max 130 Mbps (802.11n 2x2 MIMO)
Security	WEP 64/128, WPA, WPA-PSK and WPA2, TKIP and AES/CCMP, LEAP, PEAP including MS-CHAP

Classic Bluetooth	
Wireless standards (profiles)	PAN (PANU & NAP)
Operation modes	Access point or Client
Max. number of clients for Access Point	7
RF output power	14 dBm EIRP (including max antenna gain 3 dBi)
Power consumption	36 mA @ 24 VDC
Net data throughput	~1 Mbps
Bluetooth version support	Classic Bluetooth v2.1
Security	Authentication & Authorization, Encryption & Data Protection, Privacy & Confidentiality, NIST Compliant, FIPS Approved

Bluetooth Low Energy	
Wireless standards (profiles)	GATT
Operation modes	Central or Peripheral (pending)
Max. number of clients for Central	7
RF output power	10 dBm EIRP (including max antenna gain 3 dBi)
Power consumption	36 mA @ 24 VDC
Net data throughput	~200 kbps
Bluetooth version support	Bluetooth 4.0 dual-mode
Security	AES-CCM cryptography

13. Reference Guides

13.1. Wireless Technology Basics

Wireless technology is based on the propagation and reception of electromagnetic waves. These waves respond in different ways in terms of propagation, dispersion, diffraction and reflection depending on their frequency and the medium in which they are travelling.

To enable communication there should optimally be an unobstructed line of sight between the antennas of the devices. However, the so called Fresnel Zones should also be kept clear from obstacles, as radio waves reflected from objects within these zones may reach the receiver out of phase, reducing the strength of the original signal (also known as phase cancelling).

Fresnel zones can be thought of as ellipsoid three-dimensional shapes between two wireless devices. The size and shape of the zones depend on the distance between the devices and on the signal wave length. As a rule of thumb, at least 60 % of the first (innermost) Fresnel zone must be free of obstacles to maintain good reception.

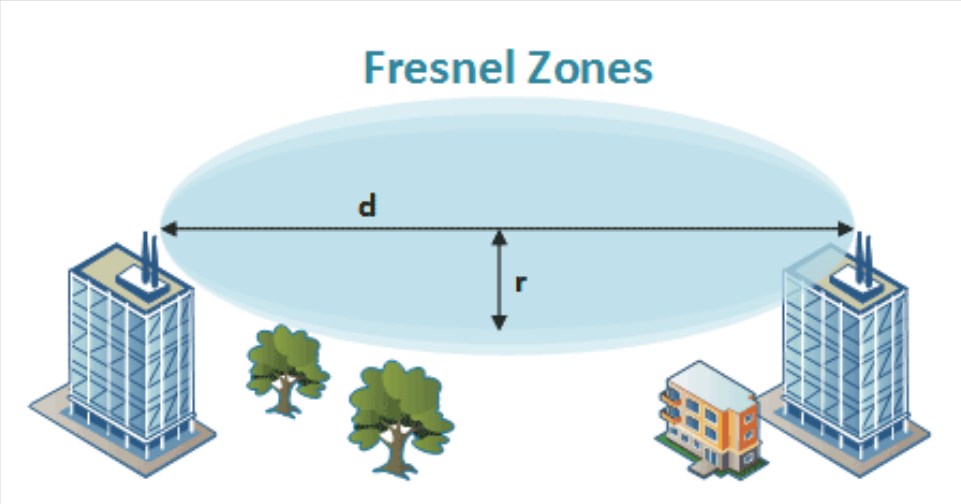


Figure 71. Fresnel zones

Area to keep clear of obstacles (first Fresnel zone)		
Distance (d)	**Fresnel zone radius (r)**	
	2.4 GHz (WLAN or Bluetooth)	**5 GHz (WLAN)**
100 m	1.7 m	1.2 m
200 m	2.5 m	1.7 m
300 m	3.0 m	2.1 m
400 m	3.5 m	2.4 m

The wireless signal may be adequate even if there are obstacles within the Fresnel zones, as it always depends on the number and size of the obstacles and where they are located. This is especially true indoors, where reflections on metal objects may actually help the propagation of radio waves. To reduce interference and phase cancelling, the transmission power of the unit may in some cases have to be reduced to limit the range.

It is therefore recommended to use a wireless signal analysis tool for determining the optimal placement and configuration of a wireless device.

13.2. Internal Antenna Characteristics

13.2.1. Internal Antenna Positions

Bridge II Ethernet has three independent quarter wave monopole antennas:

- 2.4 GHz MIMO
- 5 GHz
- 2.4 GHz

If using the unit in Bluetooth mode, the 2.4 GHz antenna is used.

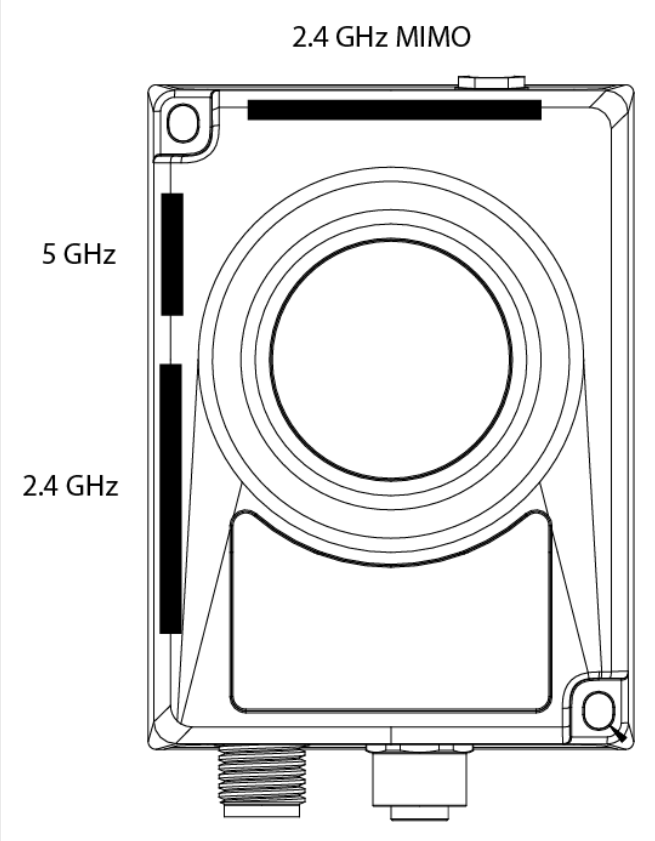
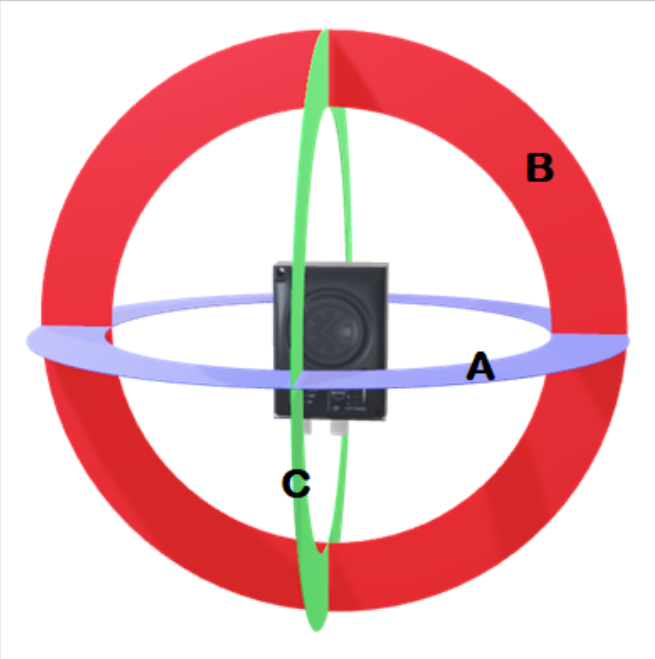


Figure 72. Placement of the three antennas in the unit

13.2.2. Lab Environment Diagrams

This topic describe the radiation measurements in different angles.



A. Azimuth plane is the horizontal spread of the radiation
B. Elevation 90° is the vertical expansion
C. Elevation 0° is the front to back expansion

The radiation diagrams show the characteristics of the different antennas as measured under laboratory test conditions.

Use the diagrams as a general guide for finding the optimal placement and orientation of the units.

The diagrams show decibel (dB) relative to the Bridge II Ethernet theoretical maximum signal strength.

The 2.4 MIMO diagrams show the WLAN usage using both the 2.4 GHz antennas simultaneously (the 2.4 GHz antenna and the 2.4 GHz MIMO antenna).

Azimuth (Horisontal) View

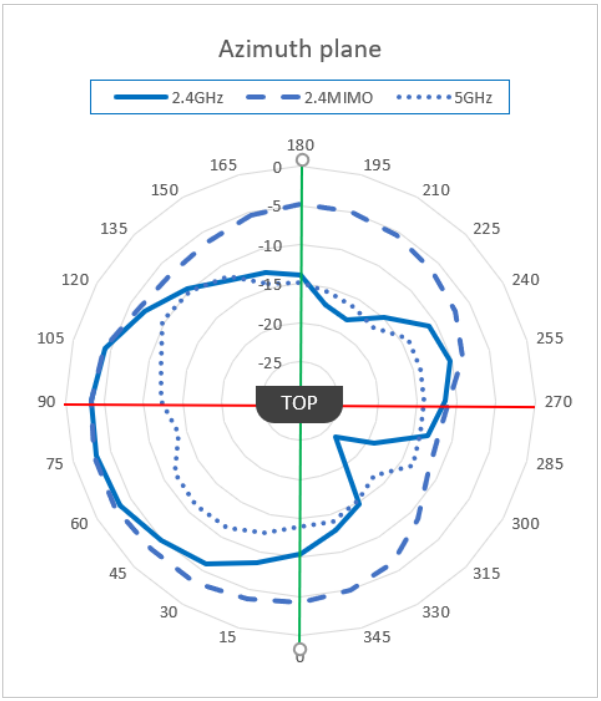


Figure 73. Azimuth plane

Front View – Elevation (Vertical)

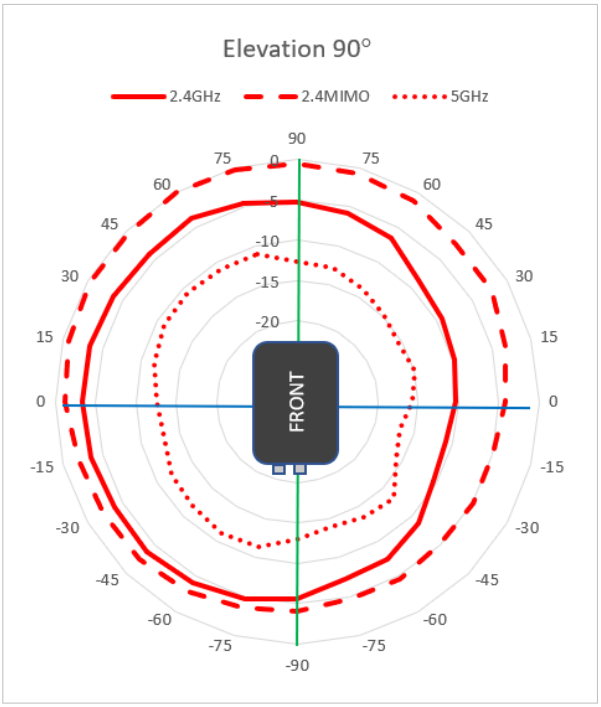


Figure 74. Elevation 90°

Side View – Elevation (Vertical)

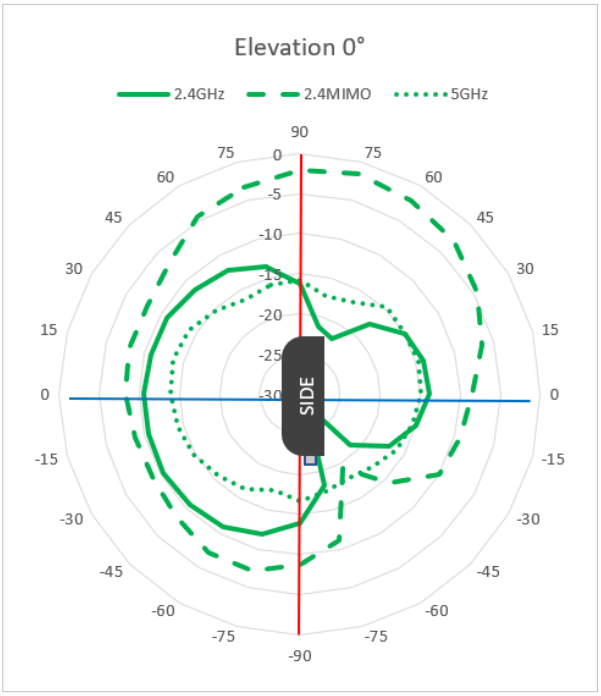


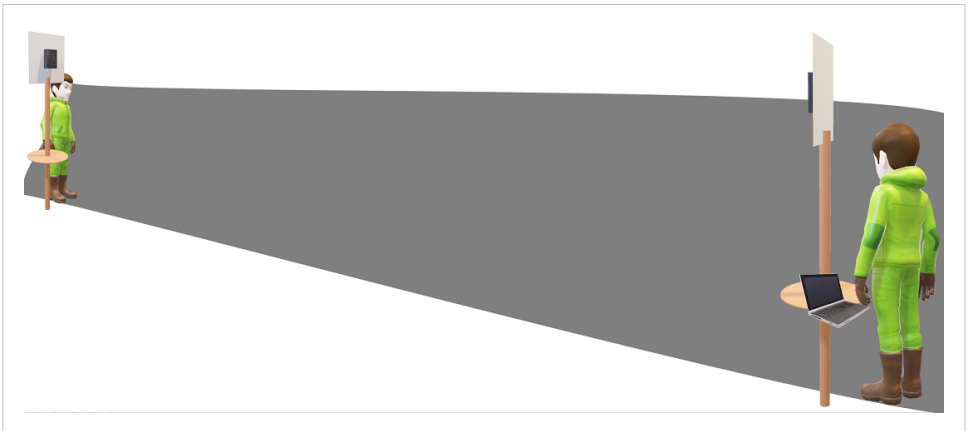
Figure 75. Elevation 0°

13.2.3. Real World Measurements

Azimuth (Horisontal) View with and without Back Shield

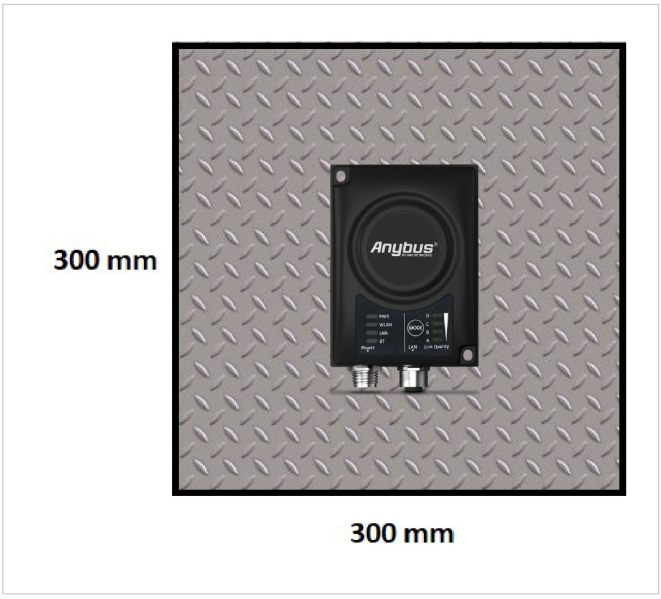
This pattern was measured in an outdoor environment, on an open field with no disturbing equipment or radiation.

As such it describes how the radio coverage can vary in a real world application.



The measurements were set up according to the graphic

Figure 76. Measurements set up



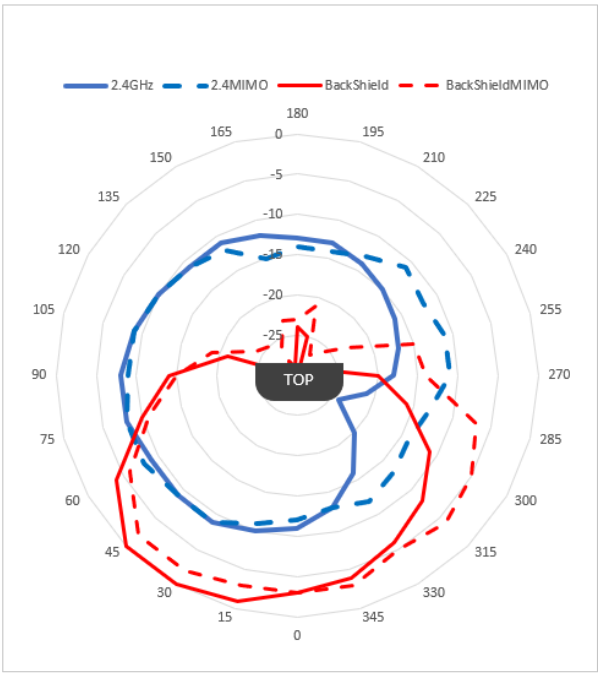
In this example, the measurements are made both with and without back shield.

A back shield is a metal surface of at least 300x300 mm.

The Bridge II Ethernet is placed in the center of the back shield.

The back shield could be any flat metal surface, like a metal plate or a metal cabinet.

Figure 77. Back shield



The measurements with back shield clearly shows that the back shield makes it possible to focus the radio energy in any desired direction (away from the back shield).

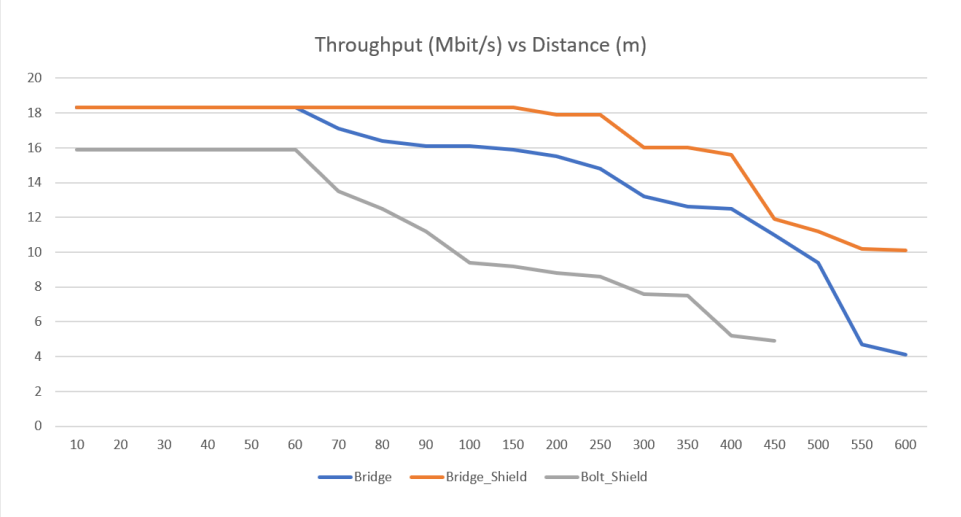
Figure 78. Measurements with and without back shield

Throughput Diagram

The diagram shows how data throughput decreases as the distance increases.

Note the huge difference between using a back shield to focus the radio energy, and not using a back shield.

Used properly, a back shield can significantly increase radio coverage.



The diagram covers both the Anybus Wireless Bridge and the Anybus Wireless Bolt.

Figure 79. Throughput diagram

Voith Group
St. Pöltener Str. 43
89522 Heidenheim, GERMANY

Phone: + 49 7951 32 1666
E-mail: Industry.Service@voith.com
Internet: www.voith.com