Einbau- und Betriebsanleitung

(Original Einbau- und Betriebsanleitung)

OnSens.SmarTemp

Energieautarke Berührungslose Thermische Messeinrichtung

Version 1, 2026-05-05
3201-014141 de, Schutzklasse 0: öffentlich

Kontakt

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

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

Wenn Sie Fragen zum Produkt haben, wenden Sie sich bitte an den Kundenservice von Voith.

3201-014141 de

Dieses Dokument beschreibt den technischen Stand des Produktes zum Redaktionsschluss.

Einbau- und Betriebsanleitung / 3201-014141
de / Schutzklasse 0: öffentlich

Inhalt

1	**Einsatzmöglichkeiten, Eigenschaften der OnSens.SmarTemp**	**5**
1.1	**Verwendung, Betrieb**	**6**
2	**Funktion der OnSens.SmarTemp**	**7**
2.1	**Temperaturfühler (OnSens.SmarTemp-Sensor)**	**7**
2.2	**OnSens.SmarTemp-Blindschraube**	**8**
2.3	**Stationärer Receiver**	**8**
3	**Technische Daten**	**9**
3.1	**Temperaturfühler**	**9**
3.2	**OnSens.SmarTemp-Blindschrauben**	**11**
3.3	**Stationärer Receiver**	**12**
4	**Benutzerhinweis**	**13**
5	**Sicherheit**	**15**
5.1	**Sicherheitshinweise**	**15**
5.1.1	Aufbau der Sicherheitshinweise	15
5.2	**Bestimmungsgemäße Verwendung**	**16**
5.3	**Nicht-Bestimmungsgemäße Verwendung**	**16**
5.4	**Allgemeine Gefahrenhinweise**	**16**
5.5	**Restgefahren**	**20**
5.6	**Verhalten bei Unfällen**	**20**
5.7	**Hinweise zum Betrieb**	**20**
5.8	**Qualifikation des Personals**	**21**
5.9	**Produktbeobachtung**	**21**
6	**Installation**	**22**
6.1	**Auslieferungszustand, Lieferumfang**	**22**
6.2	**Montage – Temperaturfühler (OnSens.SmarTemp-Sensor)**	**23**
6.3	**Montage – OnSens.SmarTemp-Blindschraube**	**25**

6.4	**Montage, Anschluss Receiver**	**25**
7	**Einbinden des Receivers in die Maschinensteuerung**	**26**
7.1	**Konfiguration des Receivers**	**27**
7.1.1	HMS Receiver	27
7.1.2	Einstellung der IP-Adresse	27
7.1.3	IP-Adresse zurücksetzen	30
7.1.4	Passwort	30
7.2	**Siemens CPU**	**31**
7.2.1	Einstellung der CPU	32
7.2.2	Verwendung der OnSens.SmarTemp Voith Bibliothek	33
7.2.3	Beschreibung des Funktionsbaustein „FB20_BTM_Ablauf_Sensor_V4“	39
7.2.4	Beispiele für die Visualisierung mit WinCC	44
7.2.5	Anlage	45
7.3	**Allen-Bradley (Rockwell) CPU**	**46**
7.3.1	Importieren der kompletten Routine	46
7.3.2	Manuelle Installation der Routinen	49
7.3.3	Konfiguration der Temperatursensors und Receiver	57
7.3.4	Empfang Temperatur-Ergebnisse von Tags	58
7.3.5	Beispiel-Visualisierung mit “FT View Studio”	58
7.3.6	Anlage	60
8	**Inbetriebnahme**	**61**
9	**Wartung, Instandhaltung**	**62**
9.1	**Außenreinigung**	**63**
10	**Entsorgung**	**64**
11	**Störungen – Abhilfe, Fehlersuche**	**65**
12	**Rückfragen, Monteur- und Ersatzteilbestellung**	**68**
13	**Ersatzteilinformation**	**69**
13.1	**Temperaturfühler**	**69**
13.2	**OnSens.SmarTemp -Blindschrauben**	**70**
13.3	**Stationärer Receiver**	**70**
13.3.1	Kabel Spannungsversorgung 5 Meter	70
13.3.2	Kabel Netzwerk 5 Meter	70
14	**Anhang**	**71**

1 Einsatzmöglichkeiten, Eigenschaften der OnSens.SmarTemp

Die Energieautarke Berührungslose Thermische Messeinrichtung (OnSens.SmarTemp) ist ein Überwachungssystem für Voith-Turbokupplungen.

Das System kann zur Messung der Temperatur des Betriebsmediums von Voith Turbokupplungen der Größen **366 bis 1330** eingesetzt werden (Messbereich: -40 °C bis 200 °C).

Durch die berührungslose Signalübertragung ist es möglich, die Temperatur des Betriebsmediums im laufenden Betrieb zu messen und Rückschlüsse auf die tatsächliche Kupplungsbelastung zu ziehen.

Da die Temperaturmessung direkt im Betriebsmedium erfolgt, werden Belastungsänderungen schnell erkannt. Dadurch kann auf mögliche Überlastungen schnell reagiert und Übertemperaturen verhindert werden.

Der Verlust der Kupplungsfüllung über die Schmelzsicherungsschrauben und den damit verbundenen Ausfallzeiten können damit sicher vermieden werden.

Zu beachten ist, dass auch das OnSens.SmarTemp, wie jedes andere Temperaturmesssystem die Temperatur zeitverzögert anzeigt.
Bei der Auswertung und weiteren Verarbeitung in der Maschinensteuerung muss die Zeitverzögerung, die abhängig von der momentanen Aufheizgeschwindigkeit der Betriebsflüssigkeit ist, berücksichtigt werden.

Weiterhin kann die für den Betrieb der Maschine zur Verfügung stehende Antriebsleistung optimiert genutzt werden. Halten Sie Rücksprache mit Voith.

Nutzen und Reaktionsmöglichkeiten:

- **Temperaturwarnung**
- **Abschaltung des Antriebmotors**
- **Reduzierung der Motordrehzahl (Dieselmotoren)**
- **Reduzierung der Lastaufnahme**
- **Optimierung der Lastaufnahme der Arbeitsmaschine**

Schmelzsicherungsschrauben

Schmelzsicherungs-schrauben
→ Betriebsanleitung Turbokupplung

Die Schmelzsicherungsschrauben schützen die Turbokupplung vor Beschädigung aufgrund thermischer Überlastung.

⚠ WARNUNG

Gefahr von Personen- und Sachschäden
Weiterbetreiben der Turbokupplung nach Ansprechen einer Schmelzsicherungsschraube beschädigt die Turbokupplung.

- Beim Einsatz von OnSens.SmarTemp dürfen die Schmelzsicherungsschrauben nicht durch Blindschrauben oder durch Schmelzsicherungsschrauben mit anderen Nenn-Ansprechtemperaturen ersetzt werden.
- Nach der Abschaltung ist die Steuerung so zu verriegeln, dass kein automatischer Neustart erfolgen kann.
- Schalten Sie die Anlage, in die die Turbokupplung eingebaut ist aus und sichern Sie den Schalter gegen Wiedereinschalten.
- Stellen Sie bei allen Arbeiten an der Turbokupplung und OnSens.SmarTemp sicher, dass sich sowohl der Antriebsmotor als auch die Arbeitsmaschine im Stillstand befinden und ein Anlaufen unter allen Umständen ausgeschlossen werden kann.

maximal zulässige Temperatur
→ Betriebsanleitung Turbokupplung

- Ein Neustart darf erst durchgeführt werden, wenn die Temperatur der Turbokupplung unterhalb der maximal zulässigen Temperatur liegt, die beim Einschalten des Motors zulässig ist.

1.1 Verwendung, Betrieb

Bestimmungs-gemäße Verwendung
→ Kapitel 5.2

Die Geräte sind nur für eine sachgerechte und bestimmungsgemäße Verwendung zugelassen. Bei Zuwiderhandlungen erlischt jegliche Garantie und Herstellerverantwortung!

- Die in dieser Betriebsanleitung spezifizierten Umgebungsbedingungen sind unbedingt einzuhalten.
- Blitzschutzmaßnahmen sind durch den Betreiber zu gewährleisten.

Schmelzsicherungs-schrauben
→ Betriebsanleitung Turbokupplung

- Es ist darauf zu achten, dass an jeder Turbokupplung, an der dieses Messsystem betrieben wird, zusätzlich die erforderlichen Schmelzsicherungsschrauben verwendet werden.

Schutzabdeckung
→ Betriebsanleitung Turbokupplung

- Das Betreiben der Turbokupplung mit OnSens.SmarTemp ist nur mit einer geeigneten Schutzabdeckung zulässig.

2 Funktion der OnSens.SmarTemp

Die Energieautarke Berührungslose Thermische Messeinrichtung (OnSens.SmarTemp) besteht aus drei Hauptkomponenten:

- **Temperaturfühler OnSens.SmarTemp-Sensor)**
- **OnSens.SmarTemp-Blindschraube**
- **Stationärer Receiver**

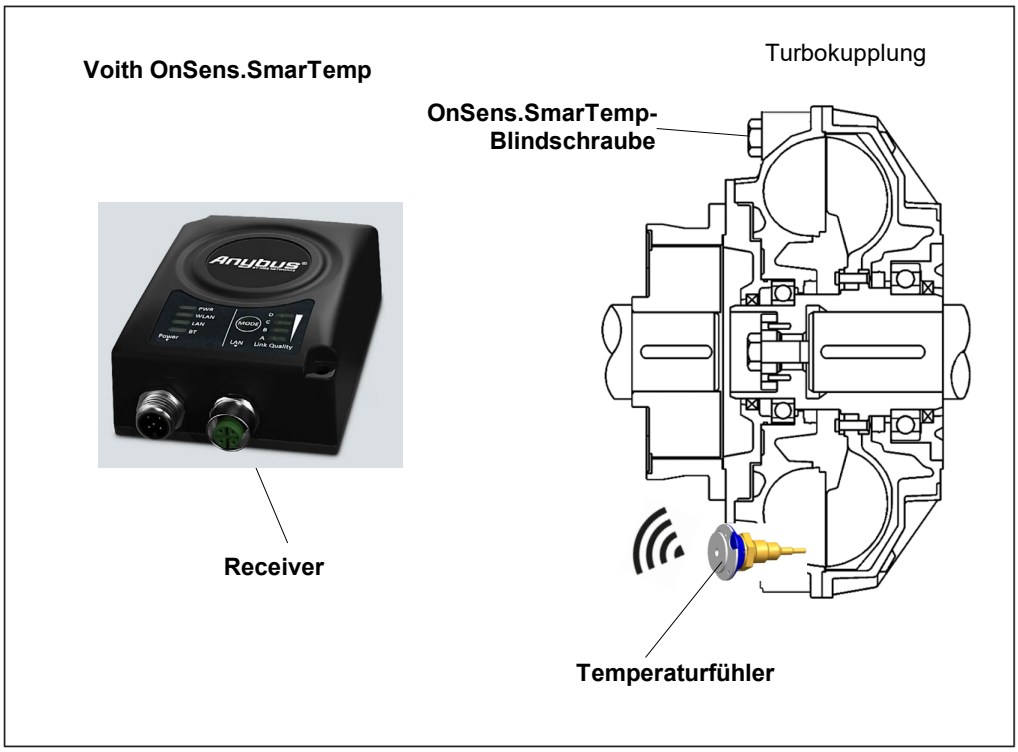


Bild 1

2.1 Temperaturfühler (OnSens.SmarTemp-Sensor)

Der Temperaturfühler ist ein energieautarkes Bauteil. Er wird in das Außenrad der Turbokupplung geschraubt und ragt mit seiner Messspitze direkt in das Betriebsmedium.

Das Messsignal wird vom Temperaturfühler berührungslos an den stationären Receiver übertragen. Die Reichweite dieses Signals ist abhängig von den baulichen Gegebenheiten am Einsatzort und beträgt typischerweise mindestens 10 Meter.

Um die Funktion des Temperaturfühlers zu gewährleisten, muss die Temperatur des Betriebsmedium der Kupplung über längere Dauer im Nennbetrieb der Anlage um mindestens ca. 20 Kelvin höher sein als die Umgebungstemperatur. Wird dieser Temperaturunterschied unterschritten (z.B. im Stillstand, Leerlaufbetrieb oder Betrieb mit geringer Last) reicht die interne Spannungsversorgung nicht aus und der OnSens.SmarTemp-Sensor sendet kein bzw. kein stabiles kontinuierliches Signal.

Da beim Start der Anlage der Temperaturfühler nicht komplett durcherwärmt ist benötigt dieser einen höheren Temperaturunterschied, bis ein stabiles Temperatursignal übertragen werden kann. Der benötigte Temperaturunterschied zwischen Betriebsmedium der Kupplung und Umgebungstemperatur beträgt in diesem instationären Betriebszustand maximal ca. 60 Kelvin.

2.2 OnSens.SmarTemp-Blindschraube

Die OnSens.SmarTemp-Blindschraube dient als Massenausgleich zum Temperaturfühler und muss zwingend genau gegenüberliegend zum Temperaturfühler eingebaut werden. Ohne OnSens.SmarTemp-Blindschraube entstehen unzulässige Kräfte durch Unwucht, die zu einer Beschädigung der Maschinenanlage führen können.

2.3 Stationärer Receiver

Der stationäre Receiver empfängt das Funksignal des Temperaturfühlers und gibt dieses an die Steuerung der Anlage weiter.

Für die Funktion des Receivers ist es notwendig diesen mit einem Kabel an einer Spannungsversorgung (9 … 30 V DC) zu verbinden. Zur Datenübertragung an die Maschinensteuerung ist ein Datenkabel notwendig. Beide Kabel sind im Lieferumfang von Voith enthalten.

Mit einem Receiver ist es möglich bis zu 7 Temperaturfühler gleichzeitig und ohne Einschränkungen zu empfangen.

Weitere Informationen zum Receiver sind im Anhang dieser Betriebsanleitung zu finden.

3 Technische Daten

3.1 Temperaturfühler

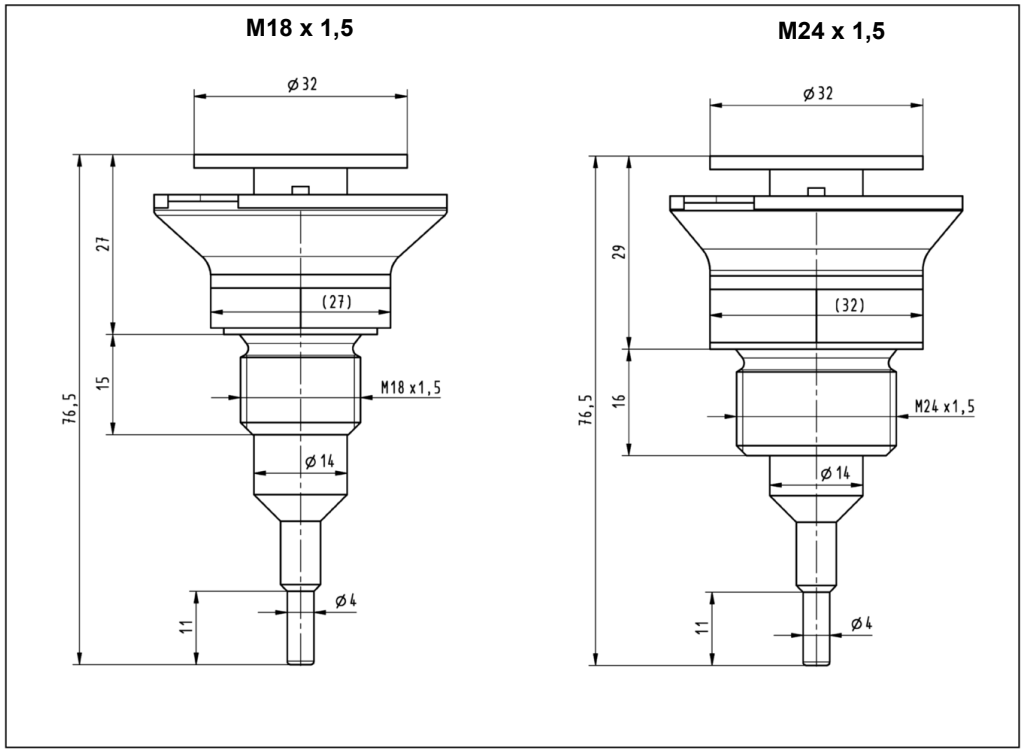


Bild 2

Für die unterschiedlichen Turbokupplungsgrößen stehen folgende Temperaturfühler zur Verfügung:

Gewindeabmessung	M18x1,5	M24x1,5
geeignet für Kupplungsgrößen	366 – 650	750 - 1330
Schlüsselweite	27	32
Anziehdrehmoment	50 Nm	144 Nm
Masse	104 ± 2 g	148 ± 2 g
Schutzart nach EN 60529	IP 65	
Messbereich	-40 °C … +200 °C	
Temperatur Betriebsmedium (kurzzeitig)	max. 200 °C	
Messtoleranz	± 2 K	
zulässige Umgebungstemperatur	-40 °C … 85 °C	
Minimale benötigte Temperaturdifferenz von Betriebsmedium zur Umgebung	> 20 K	
Reichweite Signal (abhängig von Einbaubedingungen vor Ort)	bis zu 10 m	

Tabelle 1

Der Temperaturfühler hat, wie jedes andere Temperaturmesssystem, einen Messfehler der abhängig von der Aufheizgeschwindigkeit des Betriebsmediums der Kupplung ist.

Ohne genaue Kenntnisse des Antriebs und der Turbokupplungsausführung ist eine sichere thermische Überwachung der Kupplung durch folgende Grenztemperaturen gegeben:

1. Im Nennbetrieb:

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

2. Kurzzeitig während des Anlaufs der Arbeitsmaschine oder bei Blockierung:

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

Bei genauerer Kenntnis des Antriebs und der Turbokupplung können diese Grenztemperaturen optimiert werden. Halten Sie Rücksprache mit Voith.

Formelzeichen	Bedeutung	Einheit
ϑ_{Bmax}	maximale Betriebstemperatur (dauerhaft)	°C
ϑ_{SPmax}	maximale Spitzentemperatur (kurzzeitig)	°C
ϑ_{FP}	Nenn-Ansprechtemperatur Schmelzsicherungsschrauben (siehe Turbokupplung)	°C

3.2 OnSens.SmarTemp-Blindschrauben

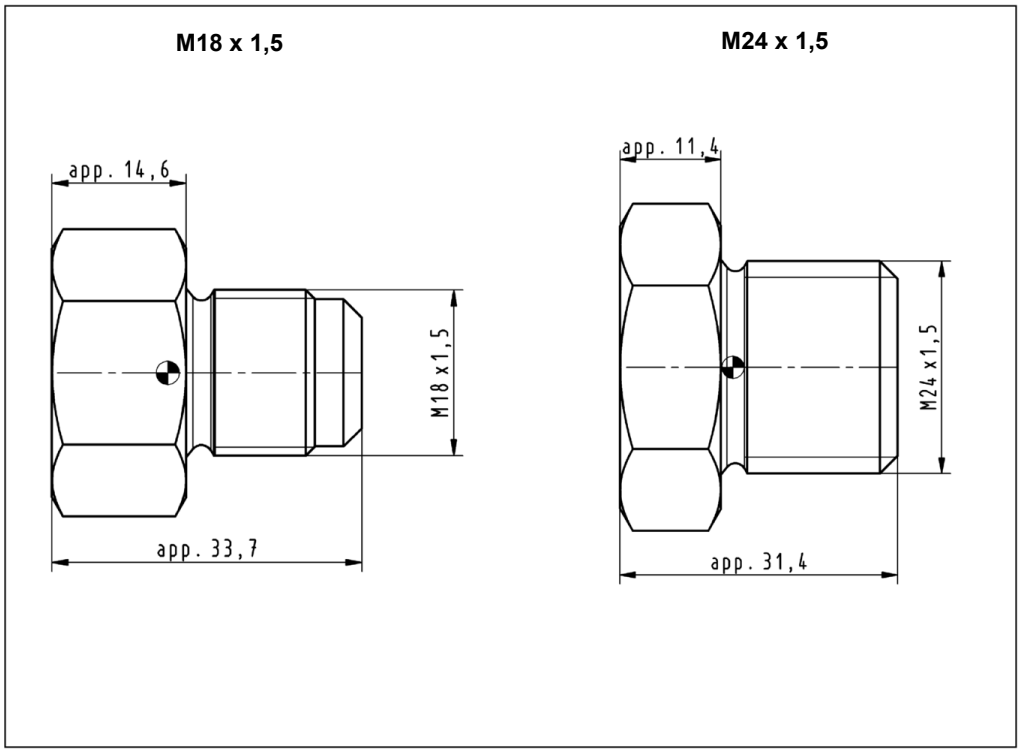


Bild 3

Für die unterschiedlichen Turbokupplungsgrößen stehen folgende OnSens.SmarTemp-Blindschrauben zur Verfügung:

Gewindeabmessung	M18x1,5	M24x1,5
geeignet für Kupplungsgrößen	366 – 650	750 – 1330
Schlüsselweite	27	32
Anziehdrehmoment	50 Nm	144 Nm
Masse	104 ± 2 g	148 ± 2 g

Tabelle 2

3.3 Stationärer Receiver

Bild 4

Funkmodul Signal	Receiver und WLAN
Schutzart nach EN 60529	IP 65
Versorgungsspannungsbereich	9 V DC… 30 V DC
Versorgungsstrom	typ. 54 mA (bei 24 V DC)
Stromaufnahme	max. 190 mA (bei 9 V DC)
max. Verlustleistung bei Nennbedingung	1,7 W
Anschlussart Spannungsversorgung	M12-Steckverbinder (A-kodiert, male)
Anschlussart Ethernet	M12-Steckverbinder (D-kodiert, female)
Max. Anzahl verbindbare Temperaturfühler	7
Zulässige Umgebungstemperatur (Betrieb)	-30 °C … +65 °C
Zulässige Luftfeuchtigkeit (Betrieb)	5 % … 93 % (keine Betauung)

Tabelle 3

Weitere Informationen zum Receiver sind im Anhang dieser Betriebsanleitung zu finden.

Passende Kabel für die Spannungsversorgung sowie Datenübertragung sind im Lieferumfang von Voith enthalten.

4 Benutzerhinweis

Diese Anleitung wird Ihnen helfen, die Berührungslose Thermische Messeinrichtung (**OnSens.SmarTemp**) sicher, sachgerecht und wirtschaftlich zu nutzen.

Wenn Sie die Hinweise in dieser Anleitung beachten, werden Sie
- die Zuverlässigkeit und die Lebensdauer der Anlage erhöhen,
- Gefahren vermeiden,
- Reparaturen und Ausfallzeiten vermindern.

Diese Anleitung muss
- ständig am Einsatzort der OnSens.SmarTemp verfügbar sein,
- von jeder Person gelesen und angewandt werden, welche die Arbeiten an der Anlage durchführt oder diese in Betrieb nimmt.

Die Berührungslose Thermische Messeinrichtung (OnSens.SmarTemp) ist nach dem Stand der Technik und den anerkannten sicherheitstechnischen Regeln gebaut. Dennoch können bei unsachgemäßer Behandlung und nicht bestimmungsgemäßer Verwendung, Gefahren für Leib und Leben des Benutzers oder Dritter, bzw. Beeinträchtigungen der Anlage und anderer Sachwerte entstehen.

Ersatzteile:
Ersatzteile müssen den von Voith festgelegten technischen Anforderungen entsprechen. Dies ist bei Originalersatzteilen gewährleistet.
Der Einbau und/oder die Verwendung von Nicht-Originalersatzteilen können die vorgegebenen Eigenschaften des **OnSens.SmarTemp** negativ verändern und dadurch die Sicherheit beeinträchtigen.
Für Schäden, die durch die Verwendung von Nicht-Originalersatzteilen entstehen, ist jegliche Haftung von Voith ausgeschlossen.

Benützen Sie für die Instandhaltung eine geeignete Werkstattausrüstung. Eine fachmännische Instandsetzung bzw. Reparatur kann nur vom Hersteller oder einer autorisierten Fachwerkstatt gewährleistet werden.

Diese Anleitung wurde mit größtmöglicher Sorgfalt erstellt. Sollten Sie dennoch weitere Informationen wünschen, so wenden Sie sich bitte an:

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

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

Die Firma Voith behält sich Änderungen vor.

5 Sicherheit

5.1 Sicherheitshinweise

In der Betriebsanleitung werden Sicherheitshinweise mit den nachfolgend beschriebenen Benennungen und Zeichen verwendet.

5.1.1 Aufbau der Sicherheitshinweise

⚠ GEFAHRENWORT
Gefahrenfolge Gefahrenquelle • Gefahrenabwehr

Gefahrenwort
Das Gefahrenwort unterteilt die Schwere der Gefahr in mehrere Stufen:

Gefahrenwort	Schwere der Gefahr
⚠ GEFAHR	Tod oder schwerste Verletzung (irreversibler Personenschaden)
⚠ WARNUNG	Möglicherweise Tod oder schwerste Verletzung
⚠ VORSICHT	Möglicherweise leichte oder geringfügige Verletzung
HINWEIS	Möglicherweise Sachschaden - des Produktes - seiner Umgebung
i INFORMATION	Nur für hilfreiche Zusatzinformationen für den sachgerechten Umgang mit dem Produkt

Tabelle 4

Gefahrenfolge
Die Gefahrenfolge nennt die Art der Gefährdung.

Gefahrenquelle
Die Gefahrenquelle nennt die Ursache der Gefährdung.

Gefahrenabwehr
Die Gefahrenabwehr beschreibt die Maßnahmen zur Abwehr der Gefährdung.

5.2 Bestimmungsgemäße Verwendung

- Die Berührungslose Thermische Messeinrichtung (OnSens.SmarTemp) dient zur berührungslosen Temperaturmessung an Voith Turbokupplungen. Eine andere oder darüberhinausgehende Verwendung, wie z.B. für nicht vereinbarte Betriebs- oder Einsatzbedingungen, gilt als nicht bestimmungsgemäß.
- Zur bestimmungsgemäßen Verwendung gehört auch das Beachten dieser Einbau- und Betriebsanleitung.
- Für Schäden, die aus einer nicht bestimmungsgemäßen Verwendung resultieren, haftet der Hersteller **nicht**. Das Risiko trägt allein der Anwender.

5.3 Nicht-Bestimmungsgemäße Verwendung

Auslegungsbereich → Betriebsanleitung Turbokupplung

- Auslegungsbereich wird nicht eingehalten.
- Eine andere, oder darüberhinausgehende Verwendung, wie z. B. für höhere Leistungen, höhere Drehzahlen oder für nicht vereinbarte Betriebsbedingungen, gilt als nicht bestimmungsgemäß.
- Weiterhin dürfen keine OnSens.SmarTemp von Drittanbietern eingesetzt werden.

5.4 Allgemeine Gefahrenhinweise

Beachten Sie bei allen Arbeiten an der Berührungslosen Thermischen Messeinrichtung die örtlichen Vorschriften zur Unfallverhütung sowie die Vorschriften zur Errichtung elektrischer Anlagen!

Gefahren während dem Arbeiten an der Berührungslosen Thermischen Messeinrichtung:

⚠ GEFAHR

Elektrischer Schlag
Aufgrund falsch montierten oder falsch angeklemmten elektrischen Komponenten und gelösten elektrischen Verbindungen, könnten Personen einen elektrischen Schlag erhalten und sich schwer verletzen, eventuell mit tödlichen Folgen.
Falsch montierte oder falsch angeklemmte elektrische Komponenten und gelöste elektrische Verbindungen, können zu Maschinenschäden führen.

- Der Anschluss an das elektrische Versorgungsnetz muss von einer Elektrofachkraft unter Beachtung der Netzspannung und der maximalen Stromaufnahme sachgerecht ausgeführt werden.
- Die Netzspannung muss, mit der auf dem elektrischen Typenschild angegebenen Netzspannung übereinstimmen.
- Netzseitig muss eine entsprechende elektrische Absicherung vorhanden sein.

Elektrischer Schlag:

⚠ GEFAHR

Elektrostatische Vorgänge
Durch statische Aufladung könnte eine Person einen elektrischen Schlag erhalten.

- Installation der Anlage, in die die Turbokupplung eingebaut ist, durch eine Elektrofachkraft.
- Maschine und Elektroinstallation haben Erdungsanschlüsse.

Arbeiten an der Turbokupplung:

⚠ WARNUNG

Verletzungsgefahr
Während dem Arbeiten an der Turbokupplung besteht Verletzungsgefahr durch Schneiden, Einklemmen, Verbrennungen und bei Minusgraden durch Kälteverbrennungen.

- Beachten Sie die Einbau- und Betriebsanleitung der Turbokupplung!
- Berühren Sie die Turbokupplung niemals ohne Schutzhandschuhe.
- Beginnen Sie mit den Arbeiten erst, nachdem die Turbokupplung abgekühlt ist.
- Sorgen Sie während den Arbeiten an der Turbokupplung für ausreichende Lichtverhältnisse, einen ausreichend großen Arbeitsbereich und gute Belüftung.
- Schalten Sie die Anlage, in die die Turbokupplung eingebaut ist aus und sichern Sie den Schalter gegen Wiedereinschalten.
- Stellen Sie bei allen Arbeiten an der Turbokupplung sicher, dass sich sowohl der Antriebsmotor als auch die Arbeitsmaschine im Stillstand befinden und ein Anlaufen unter allen Umständen ausgeschlossen werden kann.

Elektroschweißen in der Nähe des OnSens.SmarTemp:

HINWEIS

Sachschaden
Beschädigung von Elektronikkomponenten im Temperaturfühler und Receiver durch Nichteinhalten der Vorgaben.

- Bevor Sie mit Schweißarbeiten in der Nähe des OnSens.SmarTemp (5 m Abstand von Temperaturfühler oder Receiver) beginnen, klemmen Sie alle Leitungen vom Receiver ab

Lärm:

Schalldruckpegel
→ Deckblatt Betriebsanleitung der Turbokupplung

⚠ WARNUNG

Gehörverlust, bleibende Gehörschäden
Die Turbokupplung erzeugt im Betrieb Lärm. Liegt der A-bewertete äquivalente Schalldruckpegel $L_{PA,\ 1m}$ über 80 dB(A) kann dies zu Gehörschäden führen.

- Tragen Sie Gehörschutz.

Abspritzende und austretende Betriebsflüssigkeit:

⚠ WARNUNG

Erblindungsgefahr durch abspritzende Betriebsflüssigkeit, Verbrennungsgefahr
Im Falle einer thermischen Überlastung der Turbokupplung sprechen die Schmelzsicherungsschrauben an. Über diese Schmelzsicherungsschrauben tritt die Betriebsflüssigkeit aus.
Dies kann nur bei nicht bestimmungsgemäßer Verwendung geschehen.

Nicht-Bestimmungsgemäße Verwendung
→ Kapitel 5.3

- Personen, die sich in der Nähe der Turbokupplung aufhalten, müssen eine Schutzbrille tragen.
- Stellen Sie sicher, dass die abspritzende Betriebsflüssigkeit nicht mit Personen in Berührung kommen kann.
- Schalten Sie nach dem Abspritzen der Schmelzsicherungsschrauben den Antrieb sofort ab.
- Neben der Turbokupplung stehende elektrische Geräte müssen spritzgeschützt sein.

⚠ WARNUNG

Brandgefahr
Nach dem Ansprechen der Schmelzsicherungsschrauben kann sich das abspritzende Öl an heißen Oberflächen entzünden und einen Brand auslösen, sowie giftige Gase und Dämpfe freisetzen.

- Stellen Sie sicher, dass die abspritzende Betriebsflüssigkeit nicht mit heißen Maschinenteilen, Heizgeräten, Funken oder offenen Flammen in Berührung kommen kann.
- Nach Ansprechen der Schmelzsicherungsschrauben Antriebsmaschine sofort abschalten.
- Beachten Sie die Hinweise in den Sicherheitsdatenblättern.

⚠ VORSICHT

Rutschgefahr
Rutschgefahr durch abgespritztes Lot der Schmelzsicherungsschrauben und austretende Betriebsflüssigkeit.

- Sehen Sie eine hinreichend große Auffangwanne vor.
- Ausgetretenes Schmelzsicherungslot und Betriebsflüssigkeit unmittelbar entfernen.
- Beachten Sie die Hinweise in den Sicherheitsdatenblättern.

Drehende oder umherfliegende Teile:

⚠ WARNUNG

Gefahr von Personen- und Sachschäden
Drehende Teile, wie beispielsweise die Turbokupplung selbst und freiliegende Wellenteile, sind durch eine Schutzabdeckung vor Berührung und Einzug von losen Teilen zu schützen. Weiterhin besteht Gefahr von umherfliegenden Teilen im Falle einer Beschädigung des Temperaturfühlers.

- Betreiben Sie die Turbokupplung niemals ohne Schutzabdeckung.

5.5 Restgefahren

⚠ WARNUNG

Gefahr von Personen- und Sachschäden
Die Folgen von Missbrauch oder Fehlbedienung können Tod, schwere Verletzungen oder leichte Verletzungen sowie Sach- und Umweltschäden sein.

- Nur ausreichend qualifizierte, unterwiesene und berechtigte Personen dürfen an oder mit der Turbokupplung sowie der Berührungslosen Thermischen Messeinrichtung (OnSens.SmarTemp) arbeiten.
- Beachten Sie die Warnungen und Sicherheitshinweise.

5.6 Verhalten bei Unfällen

- Beachten Sie bei Unfällen die örtlichen Vorschriften sowie die Betriebsanweisungen und betreiberseitigen Sicherheitsmaßnahmen.

5.7 Hinweise zum Betrieb

- Werden während des Betriebs Unregelmäßigkeiten festgestellt, ist das Antriebsaggregat sofort auszuschalten.

5.8 Qualifikation des Personals

Alle Arbeiten, wie z.B. Transport, Einlagerung, Aufstellung, elektrischer Anschluss, Inbetriebnahme, Betrieb, Wartung, Instandhaltung und Reparatur dürfen nur von qualifiziertem und autorisiertem Fachpersonal ausgeführt werden.

Qualifiziertes Fachpersonal im Sinne dieser Betriebsanleitung sind Personen, die mit Transport, Einlagerung, Aufstellung, elektrischem Anschluss, Inbetriebnahme, Wartung, Instandhaltung und Reparatur vertraut sind und über die ihrer Tätigkeit entsprechender Qualifikation verfügen. Die Qualifikation muss durch Schulung und Einweisung sichergestellt werden.

Dieses Personal muss über Ausbildung, Unterweisung bzw. Berechtigung verfügen um:
- Anlagen fachgerecht und gemäß den Standards der Sicherheitstechnik zu betreiben und zu warten.
- Hebezeuge, Anschlagmittel und Anschlagpunkte fachgerecht zu benutzen.
- Medien und ihre Komponenten, z.B. Schmierfette, fachgerecht zu entsorgen.
- Sicherheitsausrüstung gemäß den Standards der Sicherheitstechnik zu pflegen und zu gebrauchen.
- Unfälle zu verhüten und Erste Hilfe zu leisten.

Anzulernendes Personal darf nur unter Aufsicht einer qualifizierten und autorisierten Person Arbeiten an der Turbokupplung sowie der Berührungslosen Thermischen Messeinrichtung (OnSens.SmarTemp) durchführen.

Das für Arbeiten an der Berührungslosen Thermischen Messeinrichtung (OnSens.SmarTemp) eingesetzte Personal muss
- zuverlässig sein,
- das gesetzlich vorgeschriebene Mindestalter haben,
- für die vorgesehenen Arbeiten geschult, unterwiesen und berechtigt sein.

5.9 Produktbeobachtung

Wir sind gesetzlich verpflichtet, unsere Produkte auch nach der Auslieferung zu beobachten.
Teilen Sie uns daher bitte alles mit, was für uns von Interesse ist. Beispielsweise:
- Veränderte Betriebsdaten.
- Erfahrungen mit der Anlage.
- Wiederkehrende Störungen.
- Schwierigkeiten mit dieser Einbau- und Betriebsanleitung.

Unsere Anschrift
→ **Seite 2**

6 Installation

⚠ WARNUNG

Verletzungsgefahr
Beachten Sie bei Arbeiten an der Berührungslosen Thermischen Messeinrichtung (OnSens.SmarTemp) insbesondere → Kapitel 5 (Sicherheit)!

- Stellen Sie vor Beginn der Installation sicher, dass die Potentialfreiheit aller Komponenten gewährleistet ist.
- Die Schmelzsicherungsschrauben schützen die Turbokupplung vor Beschädigung aufgrund thermischer Überlastung.
  Auch beim Einsatz des OnSens.SmarTemp dürfen die Schmelzsicherungsschrauben nicht durch Blindschrauben oder durch Schmelzsicherungsschrauben mit anderen Nenn-Ansprechtemperaturen ersetzt werden!
- Turbokupplung niemals ohne Schmelzsicherungsschrauben betreiben!
- Nach Montage des Temperaturfühlers ist die Schutzabdeckung um die Turbokupplung zwingend wieder anzubringen!

6.1 Auslieferungszustand, Lieferumfang

- Temperaturfühler (OnSens.SmarTemp) mit Dichtring
- OnSens.SmarTemp-Blindschraube (Ausgleichsgewicht) mit Dichtring
- Stationärer Receiver
- Kabel Spannungsversorgung, Länge: 5 Meter
- Netzwerkkabel, Länge: 5 Meter

Halten Sie im Falle eines nachträglichen Einbaus eines OnSens.SmarTemp bei folgenden Turbokupplungsgrößen Rücksprache mit Voith:

Kupplungsgröße	Herstelldatum
487	bis 2007-06
562	bis 2007-06
650	bis 2006-08
1000	bis 2005-06

Tabelle 5

6.2 Montage – Temperaturfühler (OnSens.SmarTemp-Sensor)

HINWEIS

Sachschaden
Nicht einhalten der Montagevorschriften.

- Zur Vermeidung von Beschädigungen sollte der Temperaturfühler nach dem Einbau und vor der Befüllung der Turbokupplung montiert werden.
- Anziehdrehmoment für Temperaturfühler (→ Kapitel 3.1) beachten.

- Dokumentation der MAC-Adressen aller verbauten Temperaturfühler. Diese ist auf dem Temperaturfühler außen graviert (12-stellig, Format: xx-xx-xx-xx-xx-xx)
- Den Temperaturfühler mit dem Dichtring anstelle einer Blindschraube in das Außenrad (Pos. 0300) [1] der Turbokupplung schrauben. Anziehdrehmoment siehe → Kapitel 3.1.

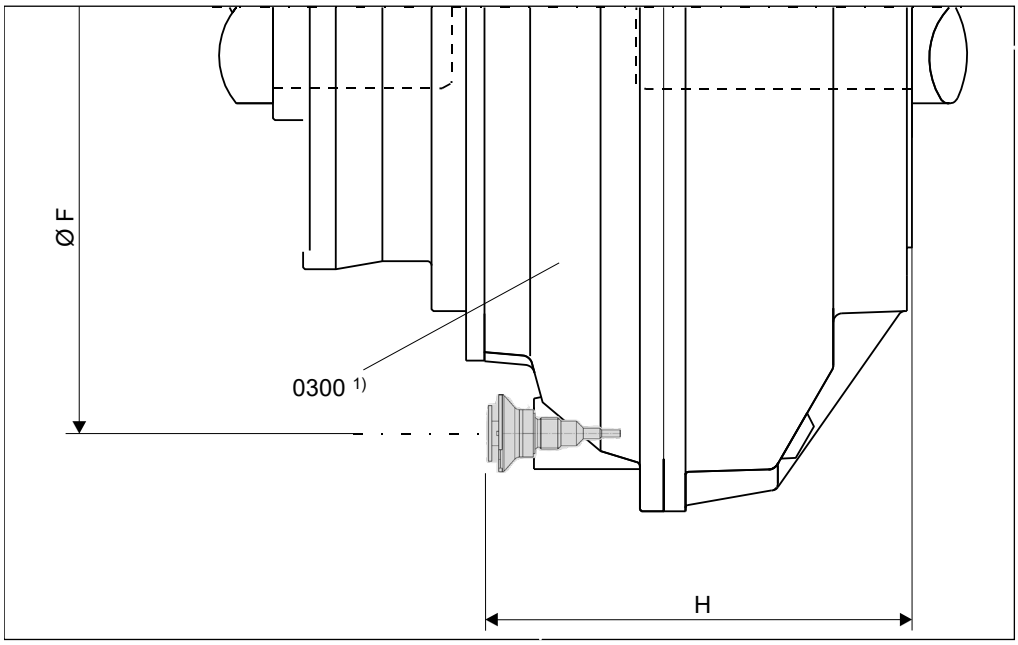


Bild 5

1) Bei Turbokupplungstyp DT ist der Einbau auch auf der gegenüberliegenden Außenradseite möglich.

Einbauabmessungen für Temperaturfühler (OnSens.SmarTemp-Sensor):

	Außenradseite	
Turbokupplungstyp	**Teilkreisdurchmesser Ø F [mm]**	**Abstand ~ 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

Tabelle 6

Die Einbaumaße von abweichenden Anordnungen sind dem Einbauplan der Turbokupplung zu entnehmen.

6.3 Montage – OnSens.SmarTemp-Blindschraube

⚠ WARNUNG

Gefahr von Personen- und Sachschäden
Unzulässige Unwucht.
- Immer OnSens.SmarTemp-Blindschraube verwenden.

- Gegenüberliegende Kupplungs-Blindschraube durch OnSens.SmarTemp-Blindschraube mit Dichtring ersetzen. Anziehdrehmoment siehe → Kapitel 3.1.

6.4 Montage, Anschluss Receiver

HINWEIS

Sachschaden
Nichteinhalten der Montagevorschriften.
- Befestigung für Receiver hinreichend stabil ausführen (nicht im Voith-Lieferumfang enthalten)!

Beschädigung der Anlage durch nicht fachgerechte Verbindung der Elektrobauteile.
- Verwendung der beiden im Lieferumfang enthaltenen Verbindungskabel für Spannungsversorgung und Datenübertragung.
- Berücksichtigung der zul. Spannung für den Receiver (9 V DC…30 V DC)

- Den Receiver an einem geeigneten Ort, an dem die Anschlussleitungen und der Receiver vor Beschädigung und direkter Sonneneinstrahlung geschützt sind, montieren.
- Receiver möglichst nicht metallisch abschirmen (z.B. durch Einbau in einen geschlossenen Schaltschrank) um eine stabile Datenübertragung gewährleisten zu können.
- Maximale Entfernung von ca. 10 Meter zu allen zu verbindenden Temperaturfühlern berücksichtigen da die Reichweite des Signals begrenzt ist.
- Im Lieferumfang enthaltenes Datenkabel zur Maschinensteuerung verlegen.
- Im Lieferumfang enthaltenes Kabel zur Spannungsquelle (9 V DC…30 V DC, Spannungsquelle nicht im Voith-Lieferumfang enthalten) verlegen. Die braune Aderleitung entspricht dem Pluspol, die blaue Aderleitung dem Minuspol.

7 Einbinden des Receivers in die Maschinensteuerung

Der Temperaturfühler sendet ein Temperatursignal an den Receiver welches dieser an die Maschinensteuerung überträgt. Um dieses Temperatursignal von der Maschinensteuerung empfangen zu können muss der Receiver wie nachfolgend beschrieben mit dem Voith-Funktionsbaustein in die übergeordnete Maschinensteuerung eingebunden werden.

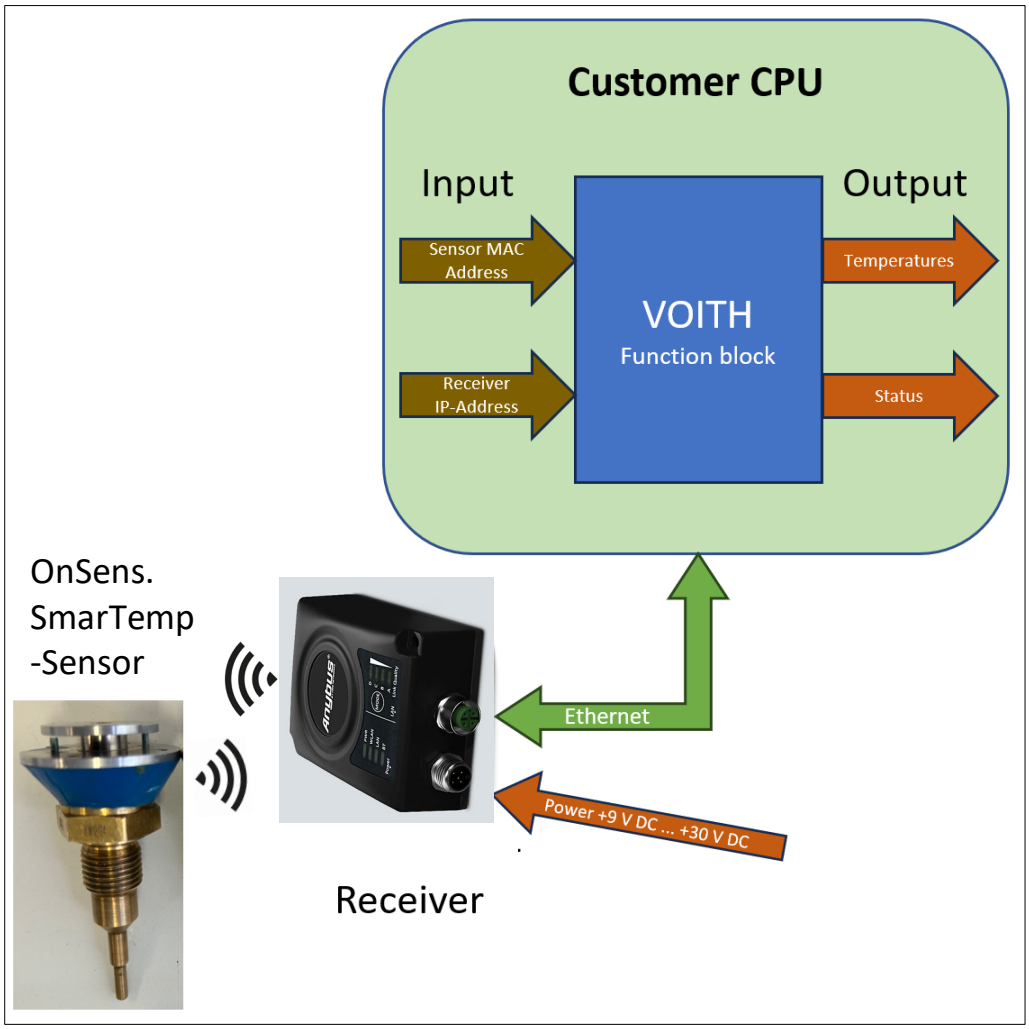


Bild 6

Bei Verwendung des Temperatursignal zur Abschaltung der Anlage ist die thermische Ansprechverzögerung des Temperaturfühlers zu berücksichtigen, siehe → Kapitel 3.1.

Um die Temperaturfühler (OnSens.SmarTemp-Sensoren) in die übergeordnete Maschinensteuerung einbinden zu können wird von jedem einzubindenden Sensor die sensorspezifische MAC-Adresse benötigt. Diese 12-stellige MAC-Adresse (Format: xx-xx-xx-xx-xx-xx) ist auf jedem Sensor graviert. Bitte halten Sie alle MAC-Adressen der einzubindenden Sensoren bereit.

⚠ WARNUNG

Gefahr von Personen- und Sachschäden
Einbindung Receiver in Kundennetzwerk

- Falls der Receiver nicht mit dem mitgelieferten Netzwerkkabel direkt an die Maschinensteuerung angeschlossen wird, sondern das Signal über das Kundennetzwerk übermittelt wird, übernimmt Voith keine Sicherheitsverantwortung für diese Datenübertragung.
- Der Kunde ist in diesem Fall für die Sicherheit und Stabilität seines Netzwerks verantwortlich.

7.1 Konfiguration des Receivers

7.1.1 HMS Receiver

Der Receiver wird mit der Werkeinstellung geliefert. Die IP-Adresse des Receivers in der Werkseinstellung lautet 192.168.0.99. Diese muss im Vorfeld mit einem beliebigen PC auf die gewünschten IP-Adresse geändert werden, falls dies notwendig ist. Weitere Informationen zum Receiver sind im Anhang dieser Betriebsanleitung zu finden.

7.1.2 Einstellung der IP-Adresse

Der Receiver muss mit Spannung versorgt werden und mit einem beliebigen PC über Ethernet-Kabel verbunden sein. Der PC muss im gleichen IP-Bereich des Receivers sein. Mit einem Standard-Browser (z.B. Microsoft Edge) können Sie das web-based-Management abrufen, indem Sie die Receiver-IP-Adresse im Browser eingeben. (Werkseinstellung: 192.168.0.99)

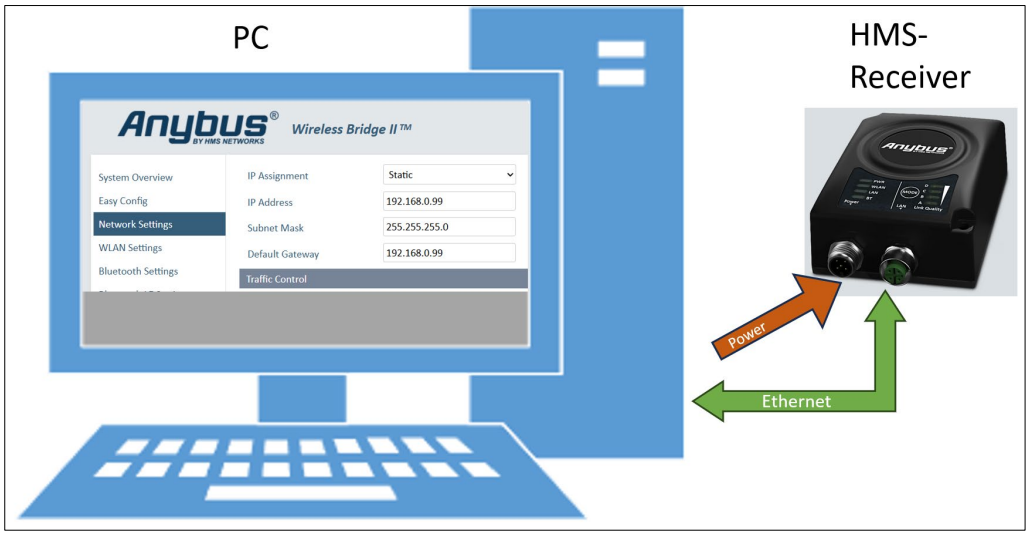


Bild 7

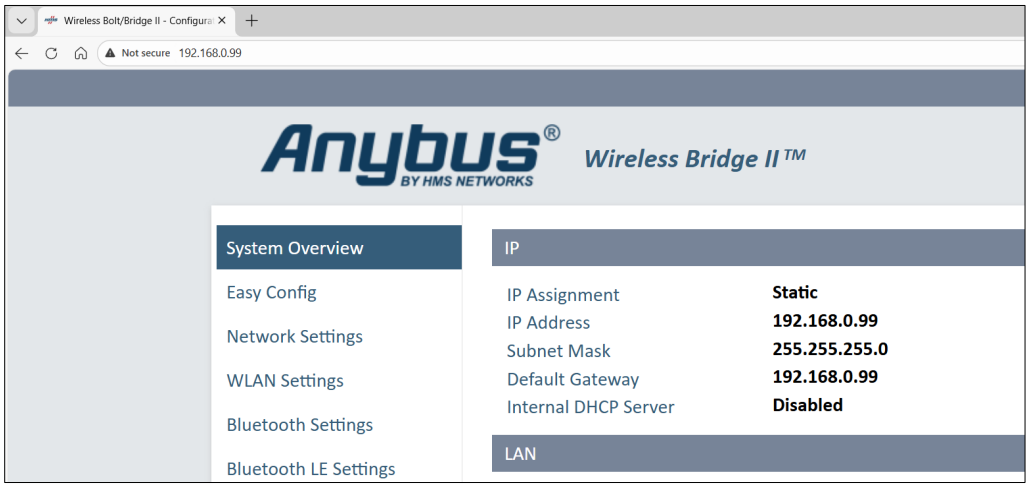


Bild 8

Gehen Sie in die Rubrik „Network Settings“

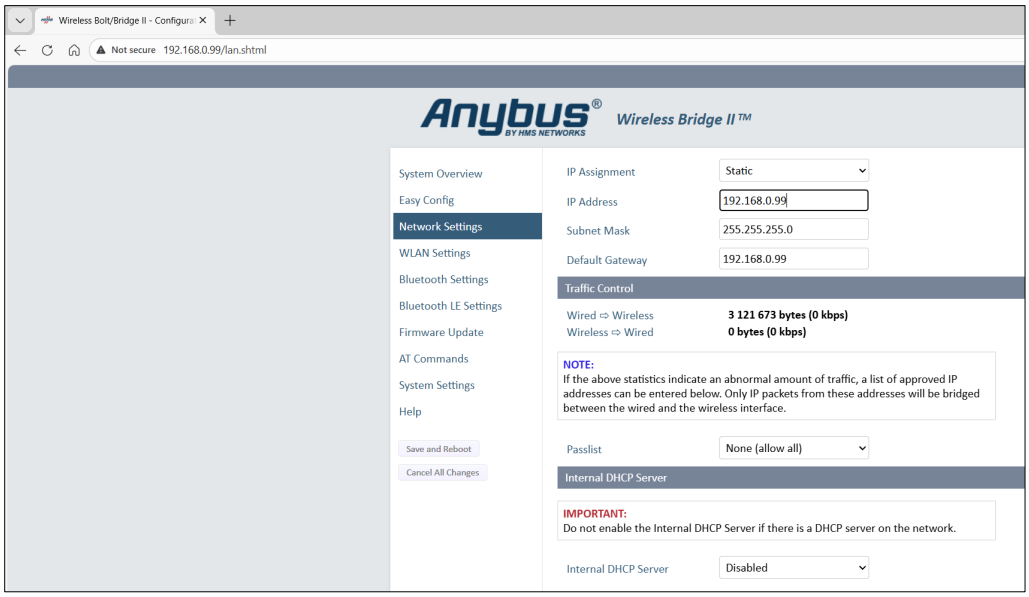


Bild 9

Dann die Gewünschte IP-Adresse eingeben, z.B. 192.168.0.251 statt 192.168.0.99.

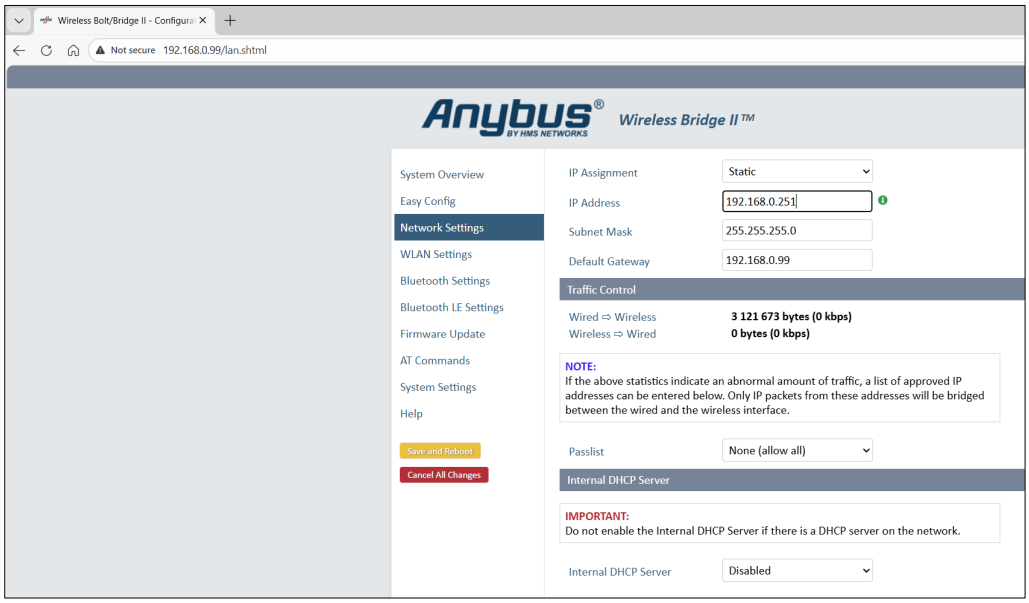


Bild 10

Dann den Button „Save and Reboot“ betätigen.

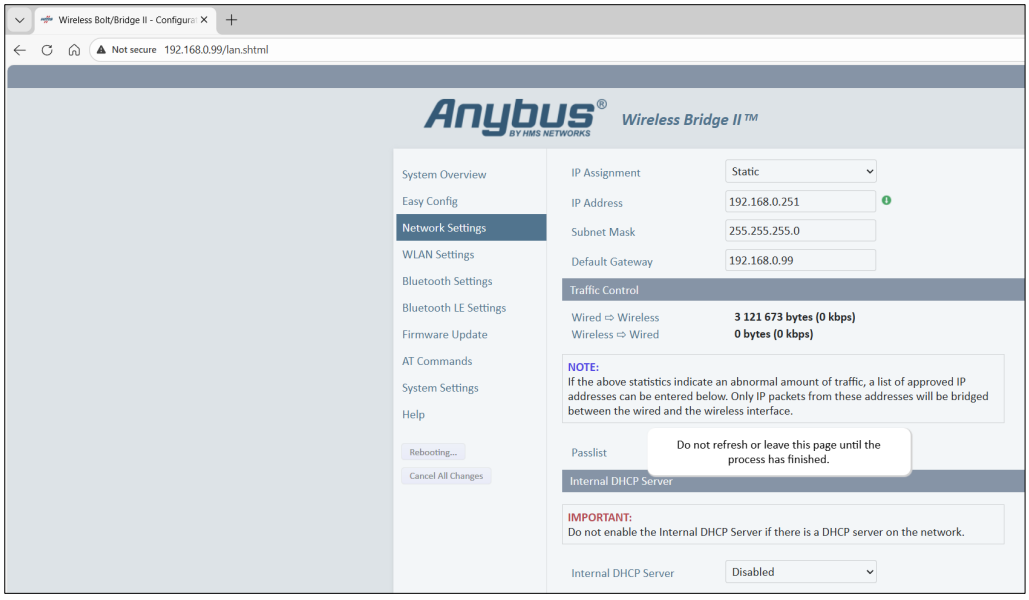


Bild 11

Nach ein paar Sekunden wird die Konfigurationsseite mit der neunen IP-Adresse automatisch aktualisiert.

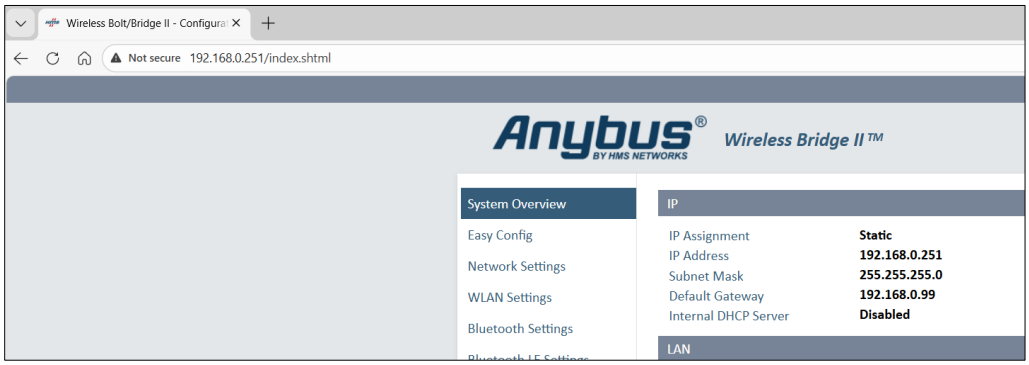


Bild 12

7.1.3 IP-Adresse zurücksetzen

Falls die IP-Adresse des Receivers nicht mehr bekannt ist, können Sie den Receiver auf Werkseinstellungen zurücksetzen. Der Receiver muss mit Spannung versorgt sein. Nachdem der Receiver vollständig gestartet ist (ca. 10 Sekunden nach dem Einschalten), drücken Sie die MODE-Taste mehr als zehn Sekunden dann lassen Sie diese los. Die IP-Adresse des Receivers wird auf 192.168.0.99 eingestellt.

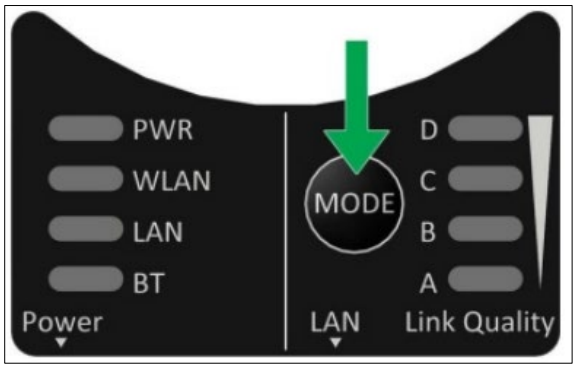


Bild 13

7.1.4 Passwort

Grundsätzlich bietet die Bedienoberfläche die Möglichkeit den Receiver mit einem Passwort zu schützen (Werkseinstellung: kein Passwortschutz).
Da der Passwortschutz aber die Kommunikation mit dem übergeordneten Funktionsbaustein beeinflusst darf der Receiver nicht mit einem Passwort geschützt werden.

Da der Receiver nur über die übergeordnete Steuerung kommuniziert ist der Passwortschutz nicht notwendig.

7.2 Siemens CPU

Der Funktionsbaustein „FB20_BTM_Ablauf_Sensor_V4“ ist für die Kommunikation mit dem Receiver (HMS) erstellt worden. Mit diesem Receiver können bis zu sieben OnSens.SmarTemp-Sensoren kommunizieren.

Dieses Kapitel gilt nur für die Steuerung Siemens CPU S7-1500.
Für die Integration in eine Steuerung vom Typ Allen-Bradley (Rockwell) CPU sind die notwendigen Informationen in Kapitel 7.3 zu finden.
Bei Verwendung einer anderen Steuerung halten Sie bitte Rücksprache mit Voith da der Funktionsbaustein nicht problemlos mit anderen Steuerungs-Modellen kompatibel ist.

Der Funktionsbaustein wurde für das TIA-Portal Version 17 erstellt.
Bei Verwendung von höheren Versionen als Version 17 muss der Funktionsbaustein hochgerüstet werden. Dieses Hochrüsten kann unter Umständen direkt beim Öffnen der Bibliothek im TIA-Portal erfolgen.
Bei Verwendung von niedrigeren Versionen als Version 17 halten Sie bitte Rücksprache mit Voith da der Funktionsbaustein nicht problemlos mit niedrigeren TIA-Portal-Versionen kompatibel ist.

Der Funktionsbaustein „FB20_BTM_Ablauf_Sensor_V4“ wird zusammen mit dieser Betriebsanleitung zur Verfügung gestellt. Bei Problemen bei der Bereitstellung oder Einbindung des Funktionsbausteins wenden Sie sich bitte an Voith.

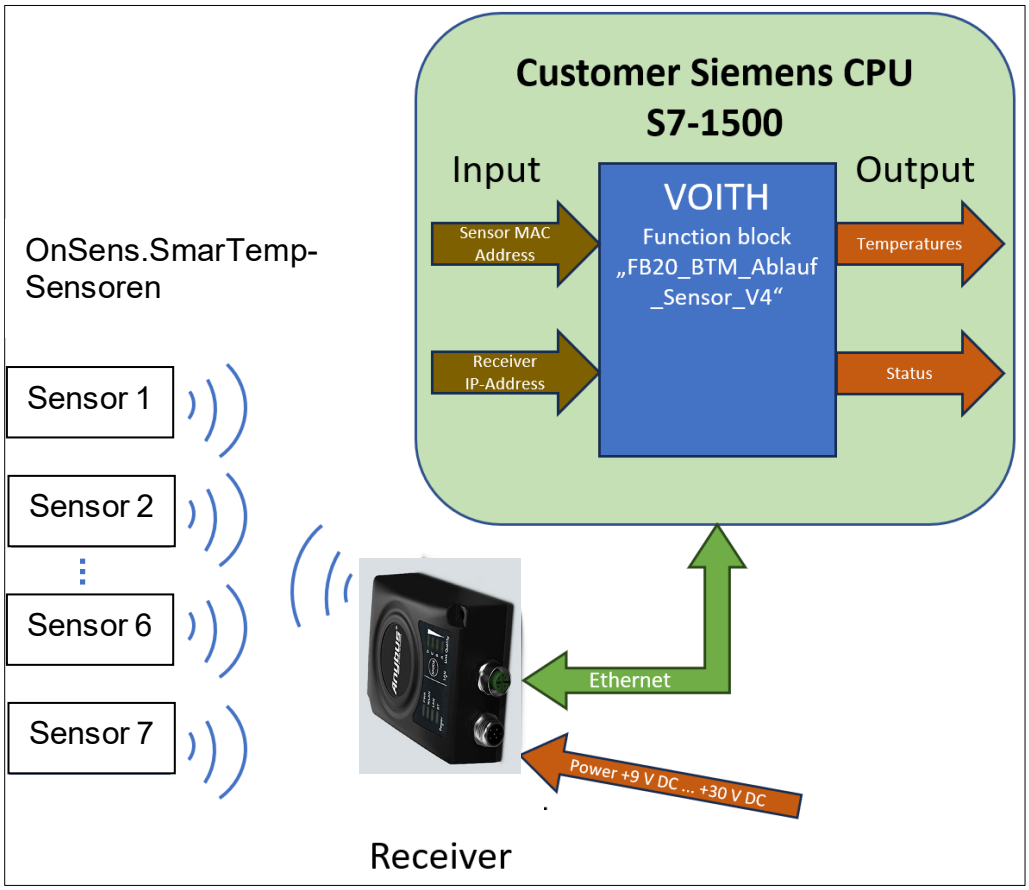


Bild 14

7.2.1 Einstellung der CPU

In der CPU sollte die Mindestzykluszeit auf 10ms eingestellt werden. Alle anderen Einstellungen der CPU können frei parametriert werden.

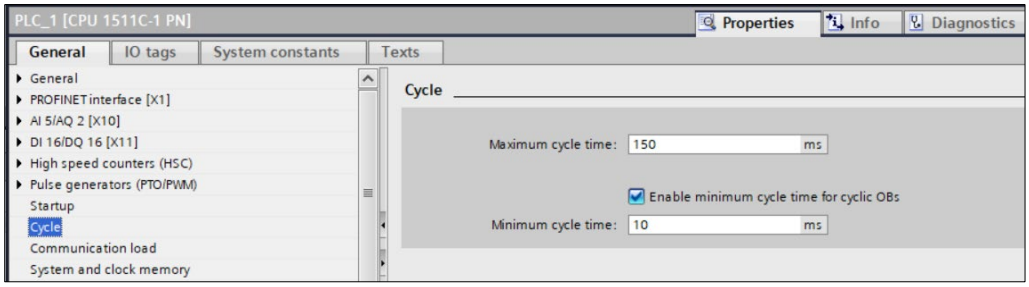


Bild 15

7.2.2 Verwendung der OnSens.SmarTemp Voith Bibliothek

Voith bietet die notwendige globale Bibliothek „BTM-Light_V4.1_xxxx-xx-xx“ für die Steuerung des Receivers. Diese wurde mit dem TIA Portal V17 erstellt.

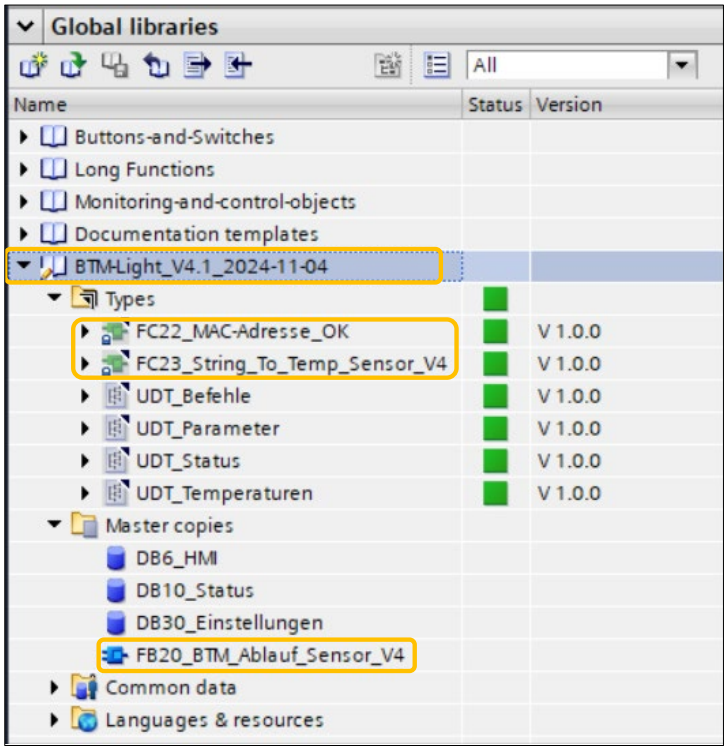


Bild 16

Die Funktionen „FC22_MAC-Adresse_OK“ und „FC23_String_To_Temp_Sensor_V4“ und der Funktionsbaustein „FB20_BTM_Ablauf_Sensor_V4“ sind mit Know-how-Schutz versehen (Copyright Voith).

7.2.2.1 Öffnen der archivierten globalen Bibliothek im TIA Portal Anlagenprojekt

1. Öffnen Sie das Anlagenprojekt
2. Klicken Sie unter „Globale Bibliotheken“ auf die Schaltfläche „Globale Bibliothek“

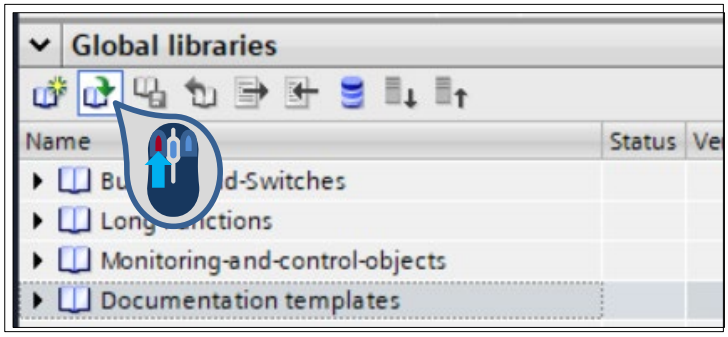


Bild 17

3. Wählen Sie im Drop-Down-Menü "Dateityp" den Eintrag "Komprimierte Bibliotheken" aus. Navigieren Sie zu der archivierten "BTM-Light_V4.1_xxxx-xx-xx.zal17" und klicken Sie auf "Öffnen".

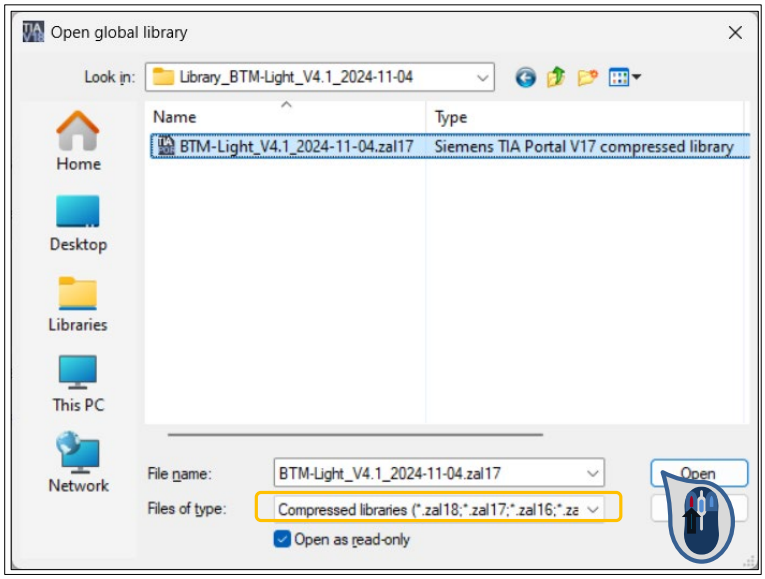


Bild 18

4. Wählen Sie den Ablagepfad für die dearchivierte "BTM-Light-Bibliothek" und bestätigen den Dialog mit "OK". Die dearchivierte "BTM-Light-Bibliothek" wird automatisch geöffnet.
5. Sollten Sie eine neuere Version von TIA Portal verwenden, wird diese Bibliothek auf die neuere TIA Portal-Version hochgerüstet. Hier z.B. von Version V17 auf Version V18.

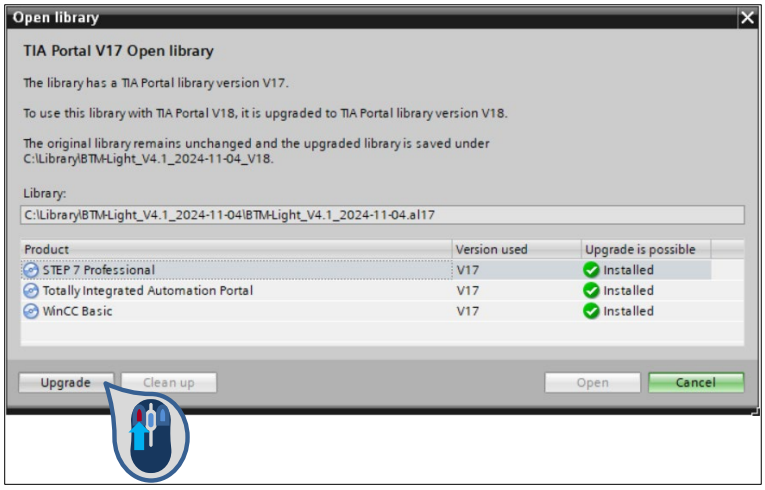


Bild 19

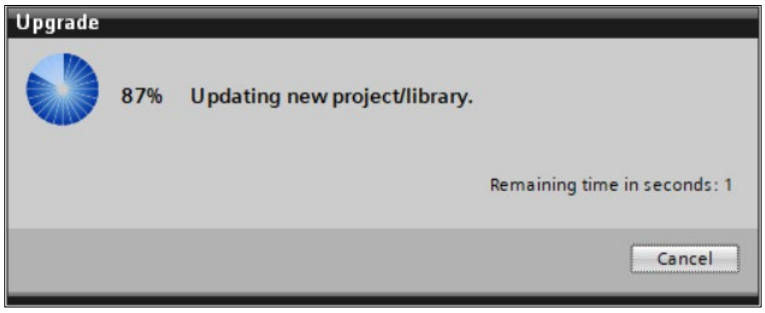


Bild 20

6. Danach wird die Bibliothek in der TIA Portal Version V18 geöffnet.

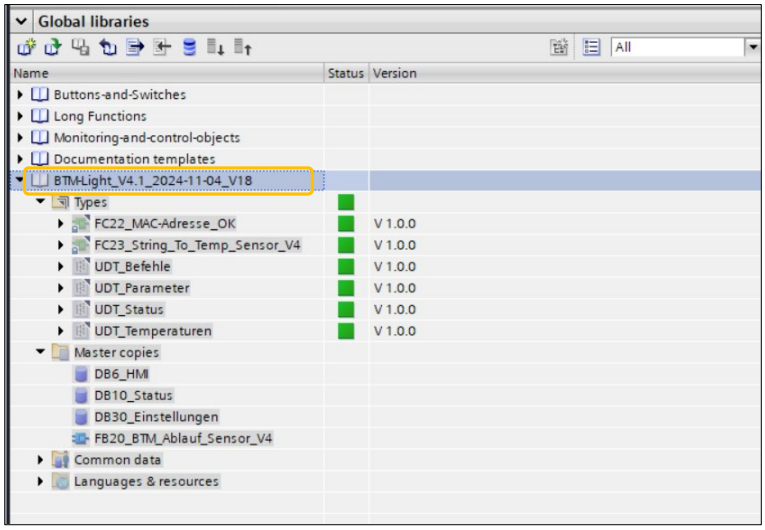


Bild 21

7.2.2.2 Einfügen von Bibliothekelementen in das Anlagenprojekt

1. Öffnen Sie Ihr Anlagenprojekt und die globale Bibliothek „BTM-Light_4.1_xxxx-xx-xx“.
2. Ziehen Sie die Bibliothekelemente (FC, FB und DB) per Drag and Drop in den Ordner „Programmbausteine“ und die Bibliothekelemente UDT in den Ordner „PLC-Datentypen“.

Bild 22

3. Fügen Sie den Funktionsbaustein „FB20_BTM_Ablauf_Sensor_V4“ per Drag and Drop in das Netzwerk des Organisationsbausteins „OB1“. Ein Instanz-Datenbaustein wird automatisch erzeugt. Geben Sie den Namen und die Nummer des Instanz-Datenbausteins ein und klicken Sie auf „OK“.

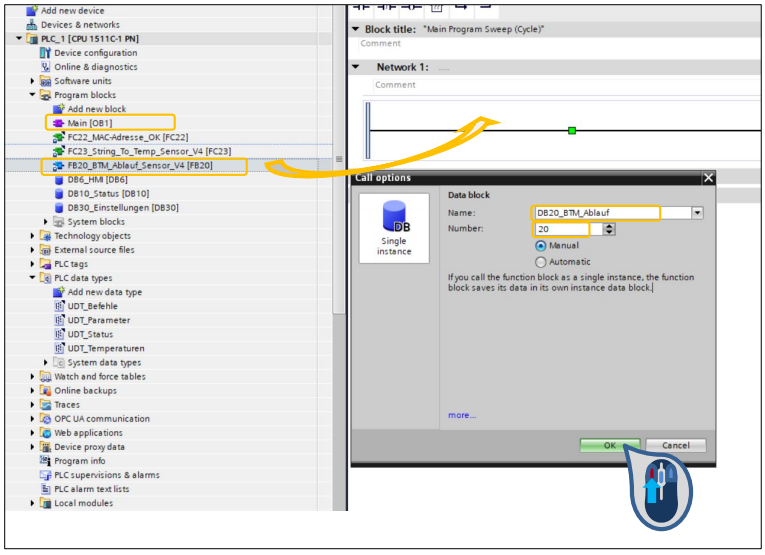


Bild 23

4. Nun werden die Instanz des Funktionsbausteins „FB20_BTM_Ablauf_Sensor_V4“ im Netzwerk vom „OB1“ und den Instanz-Datenbaustein in Ordner „Programmbausteine“ angezeigt.

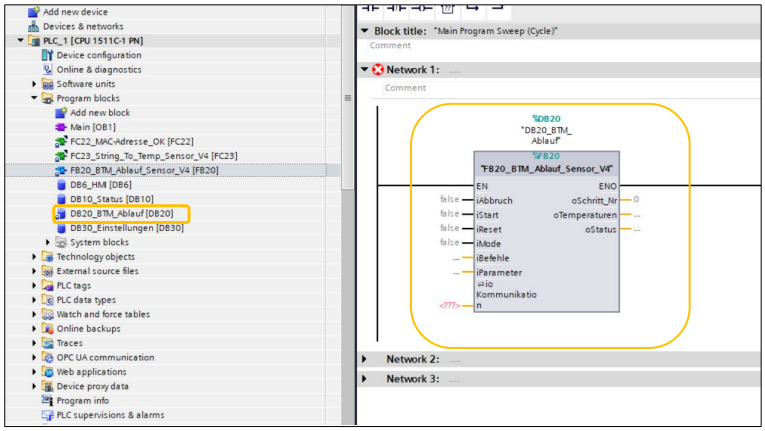


Bild 24

5. Beschalten Sie die Funktionsbausteins „FB20_BTM_Ablauf_Sensor_V4„ so wie hier gezeigt (per Drag and Drop).

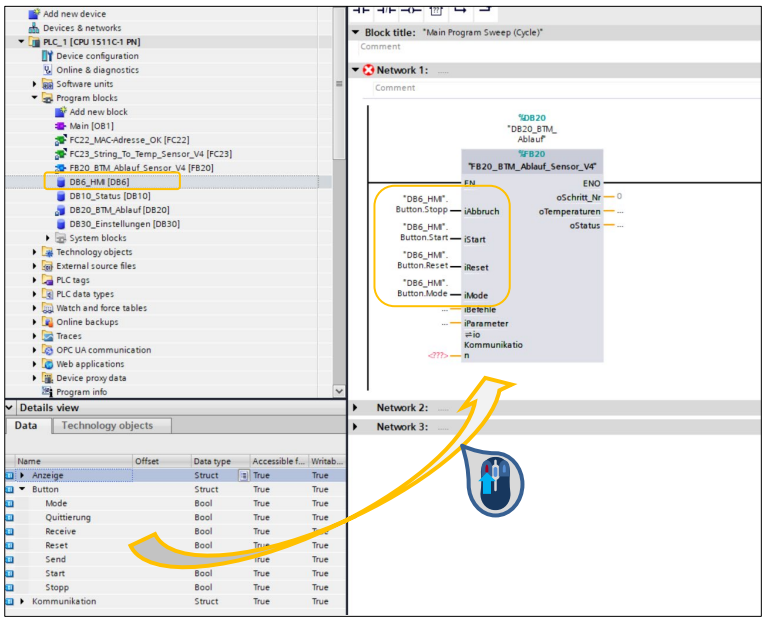


Bild 25

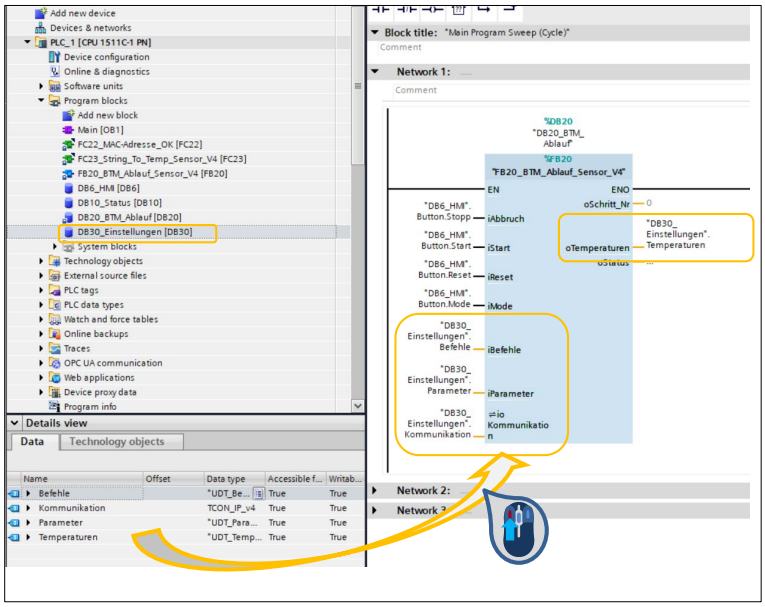


Bild 26

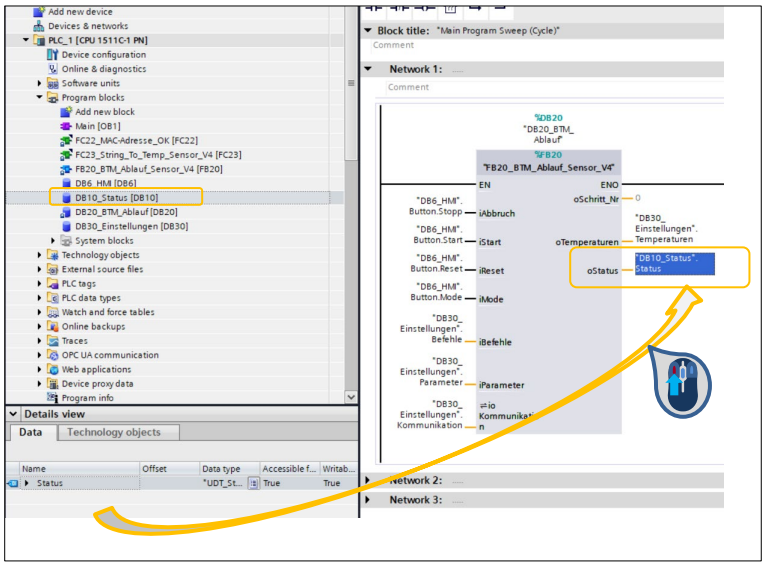


Bild 27

7.2.3 Beschreibung des Funktionsbaustein „FB20_BTM_Ablauf_Sensor_V4“

Im nachfolgenden Bild ist der Funktionsbaustein „FB20_BTM_Ablauf_Sensor_V4“ dargestellt. Dieser sollte zyklisch im „OB1“ aufgerufen werden.

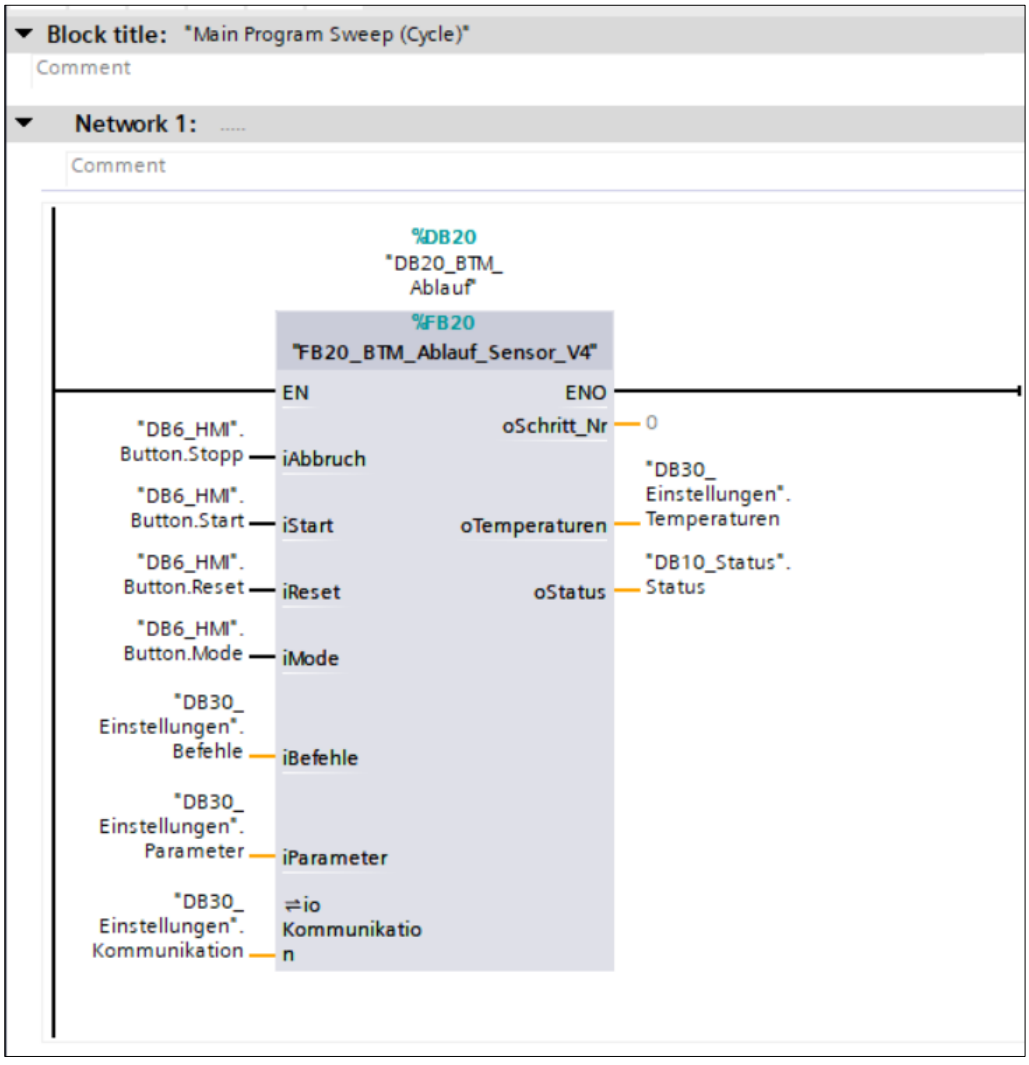


Bild 28

7.2.3.1 Parameter iAbbruch

Der Parameter iAbbruch ist als Input deklariert und vom Datentyp „BOOL“. Mit einer positiven Flanke wird die Schrittkette abgebrochen bzw. beendet.

7.2.3.2 Parameter iStart

Der Parameter iStart ist als Input deklariert und vom Datentyp „BOOL“. Mit einer positiven Flanke wird die Schrittkette gestartet.

7.2.3.3 Parameter iReset

Der Parameter iReset ist als Input deklariert und vom Datentyp „BOOL“. Mit einer positiven Flanke wird die vorhandene Verbindung der internen Bausteine „TSEND_C“ und „TRCV_C“ rückgesetzt.

7.2.3.4 Parameter iMode

Der Parameter iMode ist als Input deklariert und vom Datentyp „BOOL“. Ist der Wert des Parameters „0“, so ist der Automatikbetrieb vorgewählt. Sollte der Parameter den Wert „1“ haben, dann ist der Automatikbetrieb deaktiviert und der Nutzer kann einzelne Befehle im Testbetrieb an den Receiver senden.

7.2.3.5 Parameter iBefehle

Der Parameter iBefehle ist als Input deklariert und vom anwendungsspezifischen Typ „UDT_Befehle“. Dieser ist für den Testbetrieb vorgesehen, damit der Nutzer einzelnen Register-Befehle zum Receiver versenden kann.

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	''	☑	☑	☑

Bild 29

7.2.3.6 Parameter iParameter

Der Parameter iParameter ist als Input deklariert und vom anwendungsspezifischen Typ „UDT_Parameter“.

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		☑	☑	☑

Bild 30

Folgende Parameter können angepasst werden:

- Register-Parameter (sollten nur durch geschultes Fachpersonal verändert werden!):
  - ATS1015: Radio Mode Receiver
  - ATS6000: Advertising Intervall Minimum
  - ATS6003: Connect Connection Intervall Minimum
  - ATS6004: Connect Connection Intervall Maximum
  - ATS6007: Connect Create Connection Timeout
- Sensor-Parameter:
  - Aktivierung Sensor x
  - MAC-Adresse zu Sensor x

Hinweis: Die Parameter dürfen nur bei ausgeschalteter Schrittkette verändert werden!

7.2.3.7 Parameter ioKommunikation

Der Parameter ioKommunikation ist als InOut deklariert und vom Typ „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"						

Bild 31

Der einzige Parameter, der vom Nutzer verändert werden darf, ist die Remote Adresse (IP-Adresse des Receivers). Alle anderen Parameter dürfen nicht verändert werden.
Hinweis: Sollte die IP-Adresse verändert werden, so ist ein Neustart der CPU erforderlich!

7.2.3.8 Parameter oSchritt_Nr

Der Parameter oSchritt_Nr ist als Output deklariert, vom Datentyp „Integer“ und gibt die aktuelle Schrittnummer des Ablaufs aus.

7.2.3.9 Parameter oTemperaturen

Der Parameter oTemperaturen ist als Output deklariert und vom anwendungsspezifischen Typ „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	☑	☑	☑

Bild 32

Der Datentyp gibt die aktuellen Temperaturen der Sensoren aus, wobei hier zwischen der Board- und Tip-Temperatur unterschieden wird. Sollte ein Sensor abgewählt sein, so sind die beiden Temperaturen mit 555.5 °C gekennzeichnet. Sollte ein Sensor angewählt, aber offline sein (z.B. aufgrund zu geringer Energie), so werden für die beiden Temperaturen die Werte 999.9 °C ausgegeben.

7.2.3.10 Parameter oStatus

Der Parameter oStatus ist als Output deklariert und vom anwendungsspezifischen Typ „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		☑	☑	☑

Bild 33

Der Datentyp gibt verschiedene Statusinformationen zum Receiver und zu den aktivierten Sensoren aus:

- Receiver:
  - Status zum Baustein TRCV_C
    - Fehler in der Kommunikation aufgetreten
    - Status der Kommunikation (siehe Hilfe im TIA-Portal)
  - Status zum Baustein TSEND_C
    - Fehler in der Kommunikation aufgetreten
    - Status der Kommunikation (siehe Hilfe im TIA-Portal)
  - Verbindung zur CPU:
    - Verbindungsfehler zum Receiver (Kabel prüfen, Receiver prüfen)
    - Verbindung Online, d.h. Verbindung zwischen CPU und Receiver in Ordnung
- Sensor x:
  - Fehler MAC-Adresse (z.B. falsche Länge, falsche Zeichen, …)
  - Verbindung Online, d.h. Sensor sendet Daten an Receiver bzw. CPU
  - Unter- bzw. Überlauf Board- und/oder Tip-Temperatur
    - Unterlauf: Temperatur kleiner gleich -41°C
    - Überlauf: Temperatur größer gleich 201°C

7.2.4 Beispiele für die Visualisierung mit WinCC

Alle Sensoren sind aktiviert.

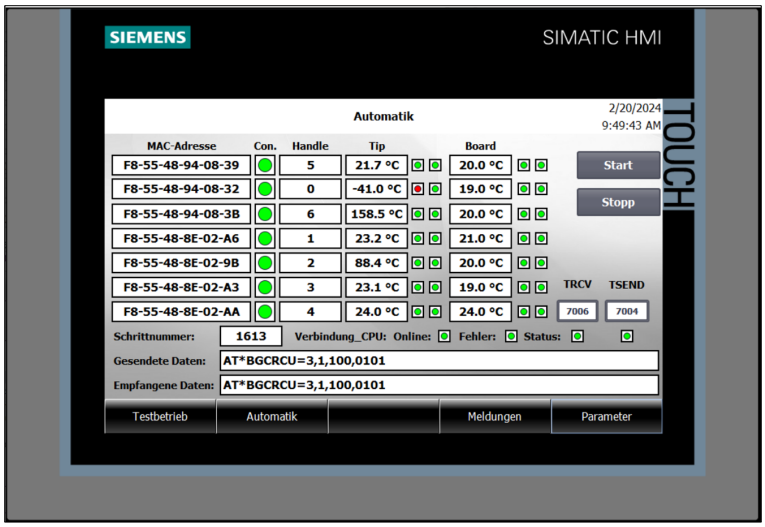


Bild 34

Der Sensor Nummer 2 ist deaktiviert (Board- und Tip-Temperatur zeigen 555,5°C).

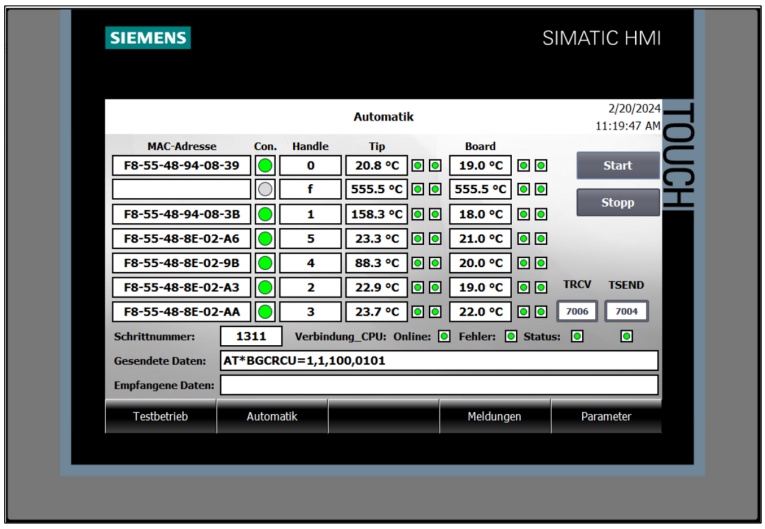


Bild 35

Eingabe der MAC-Adresse.

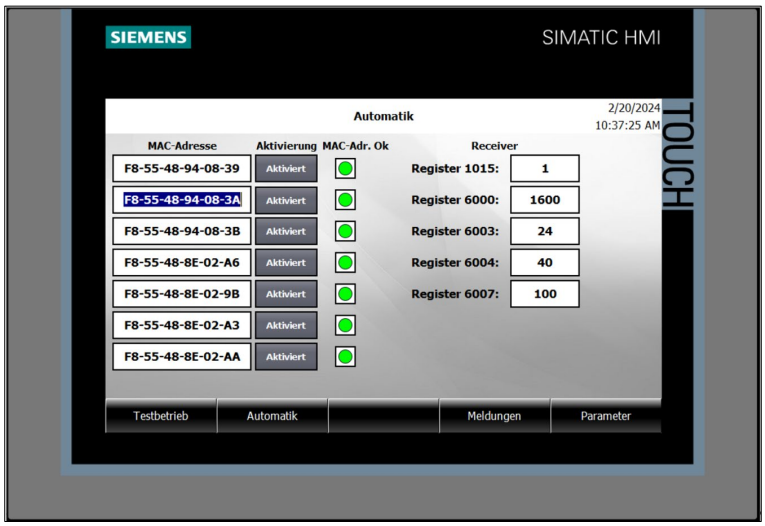
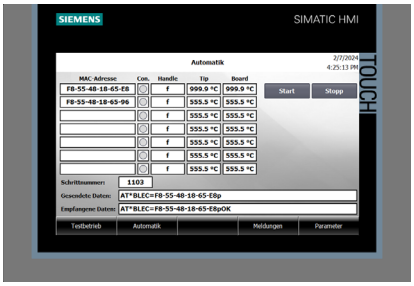
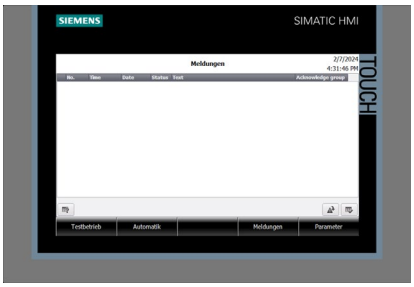


Bild 36

7.2.5 Anlage

7.2.5.1 Startprozedur

01		Hauptschalter einschalten
02		Warten, bis CPU und Visualisierung gestartet sind
02		Anstehende Störungen quittieren • Bedienbild Meldungen aufrufen • Störungen quittieren • Gegebenenfalls Störung beseitigen

7.2.5.2 Startvorrausetzung

Folgenden Voraussetzungen müssen erfüllt sein, damit der Automatikbetrieb erfolgen kann:

- Mindestens 1 Sensor aktiviert
- Kein Firewall zwischen CPU und Receiver
  100 Meter pro Segment ist die maximale Länge des LAN-Kabels
  Das LAN-Kabel muss geschirmt sein und mindestens Cat5 (100 Mbit/s) entsprechen
- Kein Fehler bei der Eingabe der MAC-Adressen
- Automatikbetrieb vorgewählt
- Keine Störung aktiv

7.3 Allen-Bradley (Rockwell) CPU

Abhängig vom Kenntnisstand des Anwenders gibt es zwei Arten die benötigte Logik in das Programm zu integrieren.
Einerseits können die kompletten Routinen mit allen benötigten Tags und den meisten Konfiguration mittels „plug&play“ importiert werden.
Alternativ können alle Tags und Routinen manuell erstellt und die beiden benötigten AOI importiert werden.

Bitte beachten Sie: Bei beiden Vorgehensweisen müssen keine Hardware-Informationen zu dem Programm hinzugefügt werden da die Kommunikation mittels TCP-Stack realisiert ist.
Allerdings wird ein Ethernet-Kommunikation-Device (z. B. EN2T oder ähnlich vorkonfiguriert) benötigt.
Beinhaltete Dateien:

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

7.3.1 Importieren der kompletten Routine

Das Installationspaket ist in der kompletten Routine mit dem Namen „BLE_TempSens_Routine_RLL.L5X“ beinhaltet.
Dieses Paket kann wie in den folgenden dargestellten Screenshots direkt in das vorhandene Programm importiert werden.

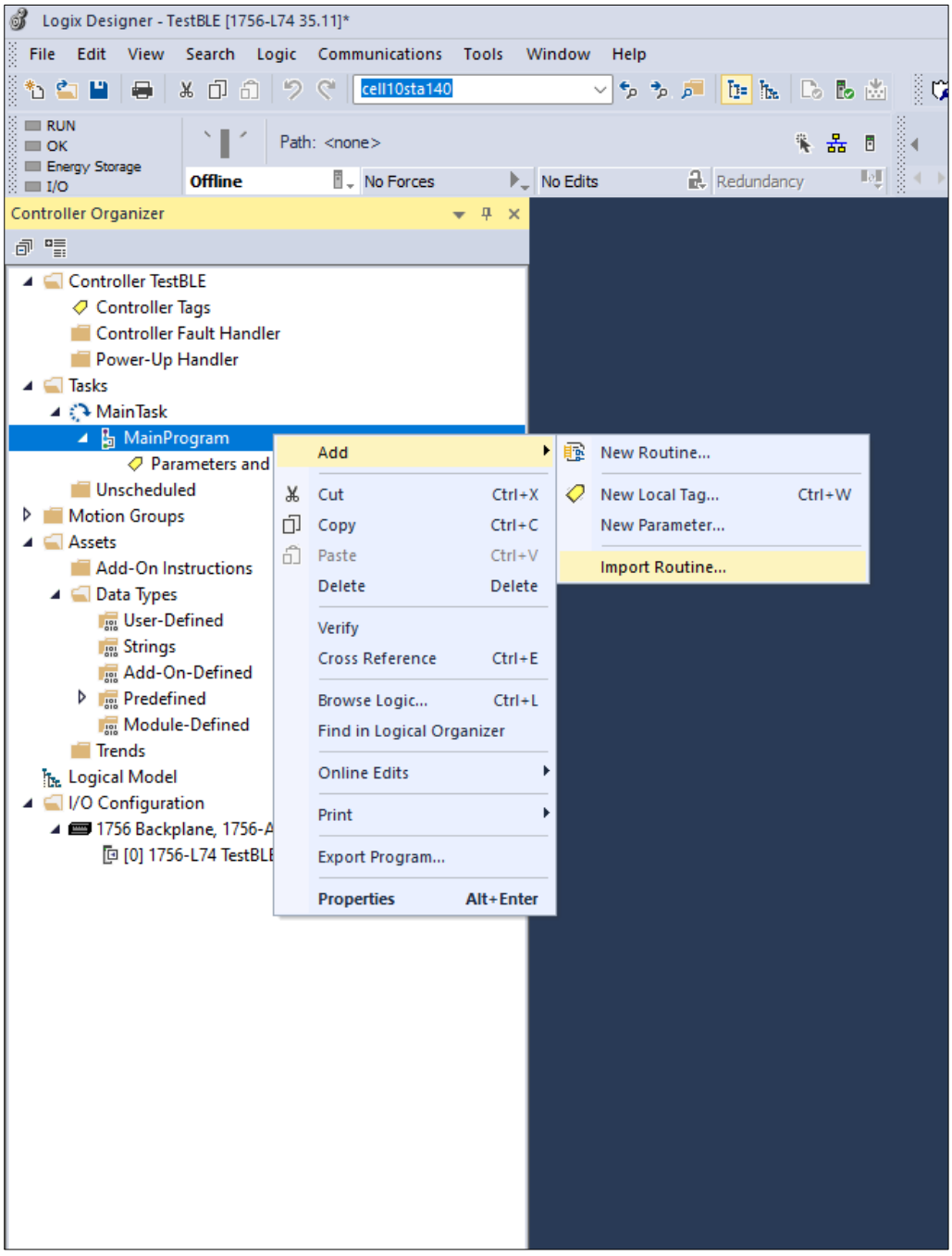

Logix Designer - TestBLE [1756-L74 35.11]*
File Edit View Search Logic Communications Tools Window Help
cell10sta140
RUN
OK
Energy Storage
I/O
Path: <none>
Offline
No Forces
No Edits
Redundancy
Controller Organizer
Controller TestBLE
Controller Tags
Controller Fault Handler
Power-Up Handler
Tasks
MainTask
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...

Bild 37

Nach dem Importieren wird die Routine mit dem Namen „BLE_TempSens“ angezeigt, in diese muss nur noch das verwendete Ethernet-Device angegeben werden.

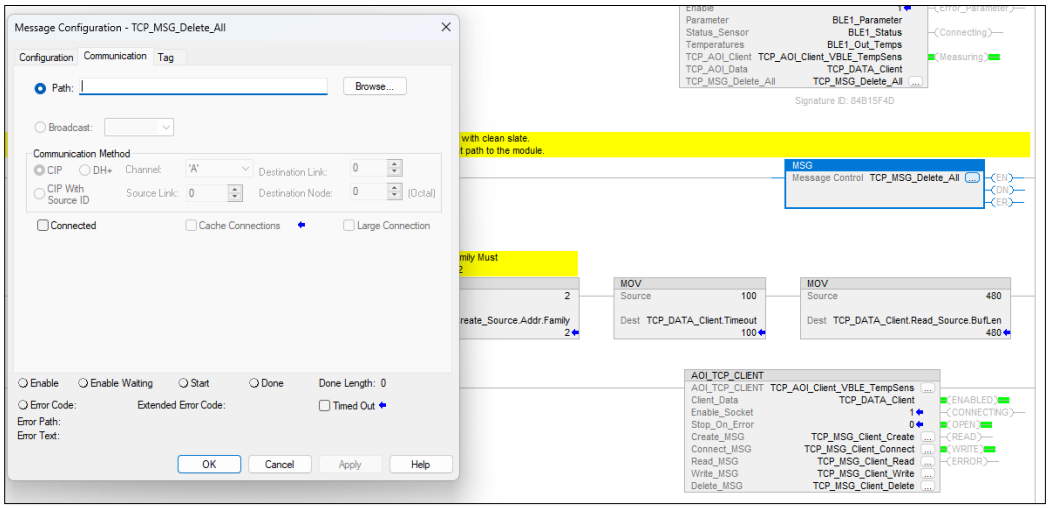


Bild 38

Es werden mehrere Meldungs-Hinweise angezeigt welche mit Klicken auf die drei Punkte neben folgenden Tag-Namen editiert werden können:

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

Durch Öffnen der Einstellungen und Navigation zum zweiten Tab muss der Pfad zum verwendeten Ethernet-Device gesetzt werden.

Danach ist die Installation abgeschlossen und das Device kann verwendet werden.

7.3.2 Manuelle Installation der Routinen

Für erfahrene Benutzer sind die zwei benötigten AOIs beinhaltet und können unter „Assets → Add On Instructions“ folgendermaßen importiert werden:

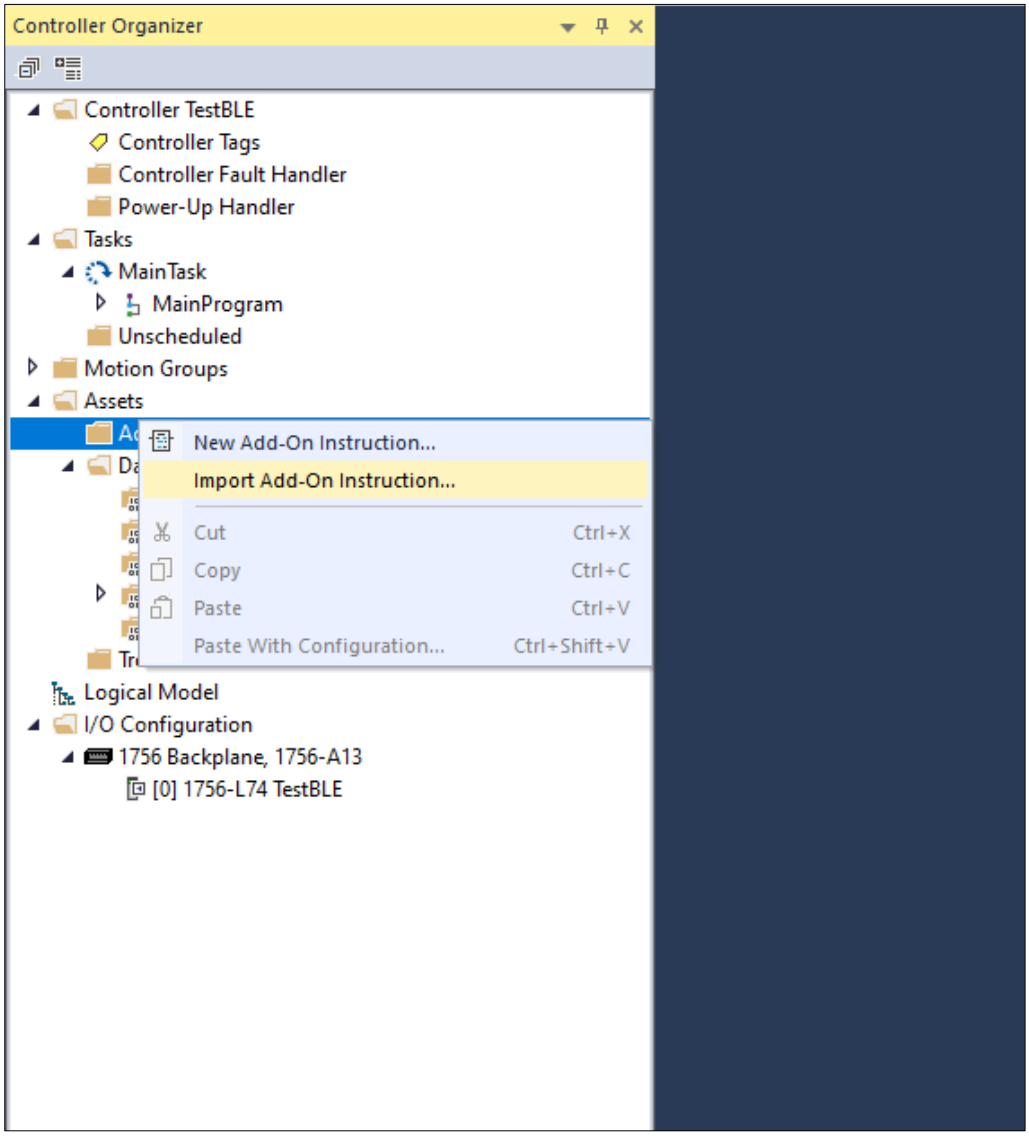


Bild 39

Damit werden alle benötigten Befehle und Datentypen zum Programm installiert. Dabei ist zu berücksichtigen, dass für den richtigen Kommunikations-Typ drei Optionen im TCP-Client-AOI gesetzt werden müssen, dargestellt in der Beispiel-Routine:

Nach Eingabe der Befehle in das Programm wird noch die Konfiguration der Meldungs-Hinweise, welche im TCP-Client beinhaltet sind, wie folgt benötigt.

7.3.2.1 Konfiguration des “Delete_All”-Befehls

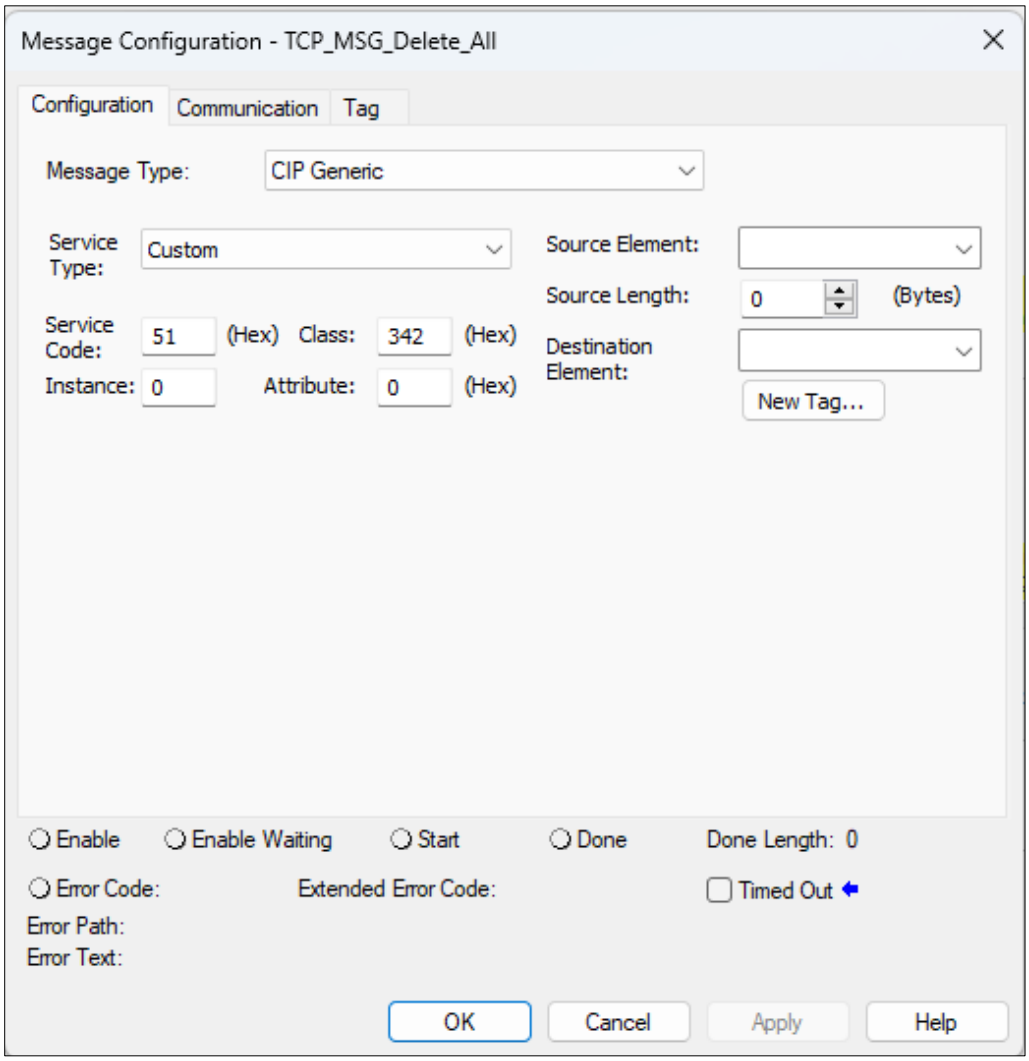


Bild 40

7.3.2.2 Konfiguration des “Create_MSG”-Befehls

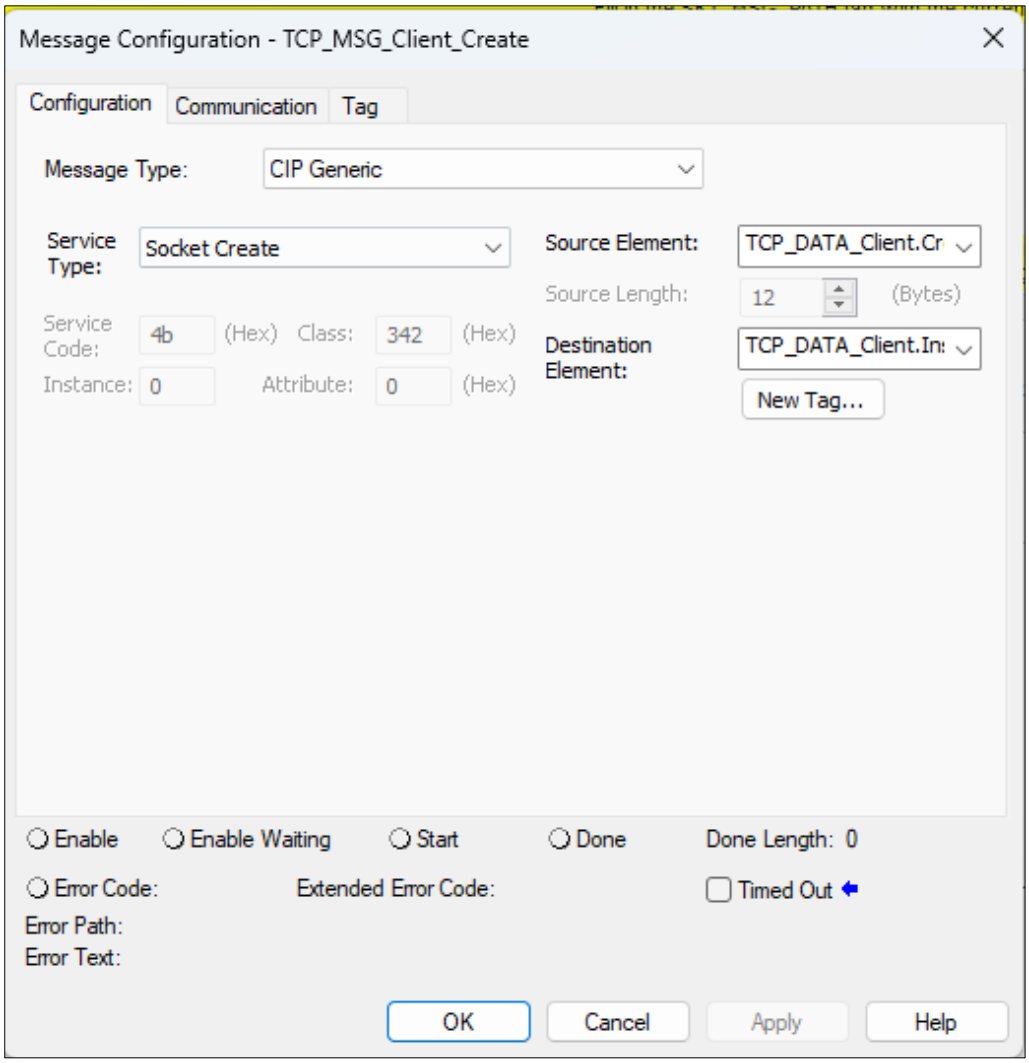


Bild 41

7.3.2.3 Konfiguration des “Connect_MSG”-Befehls

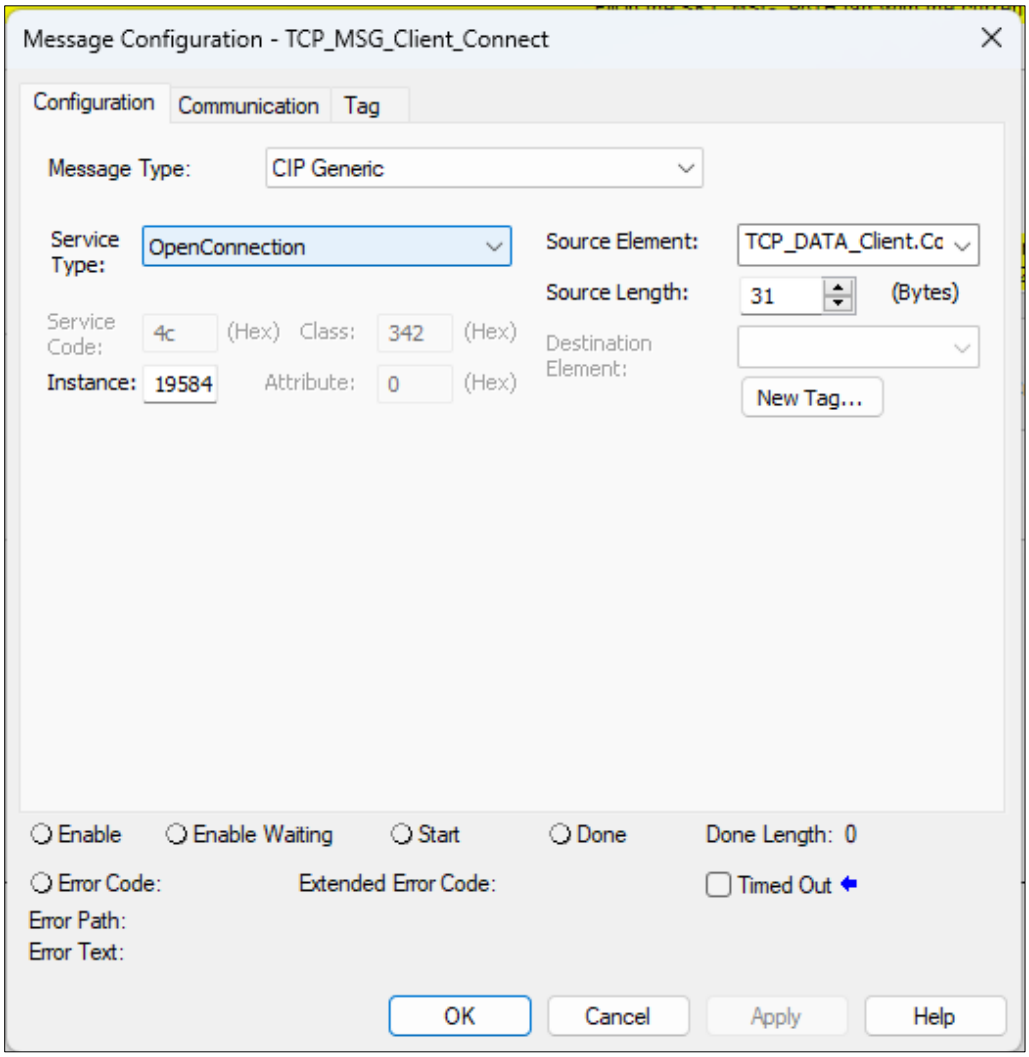


Bild 42

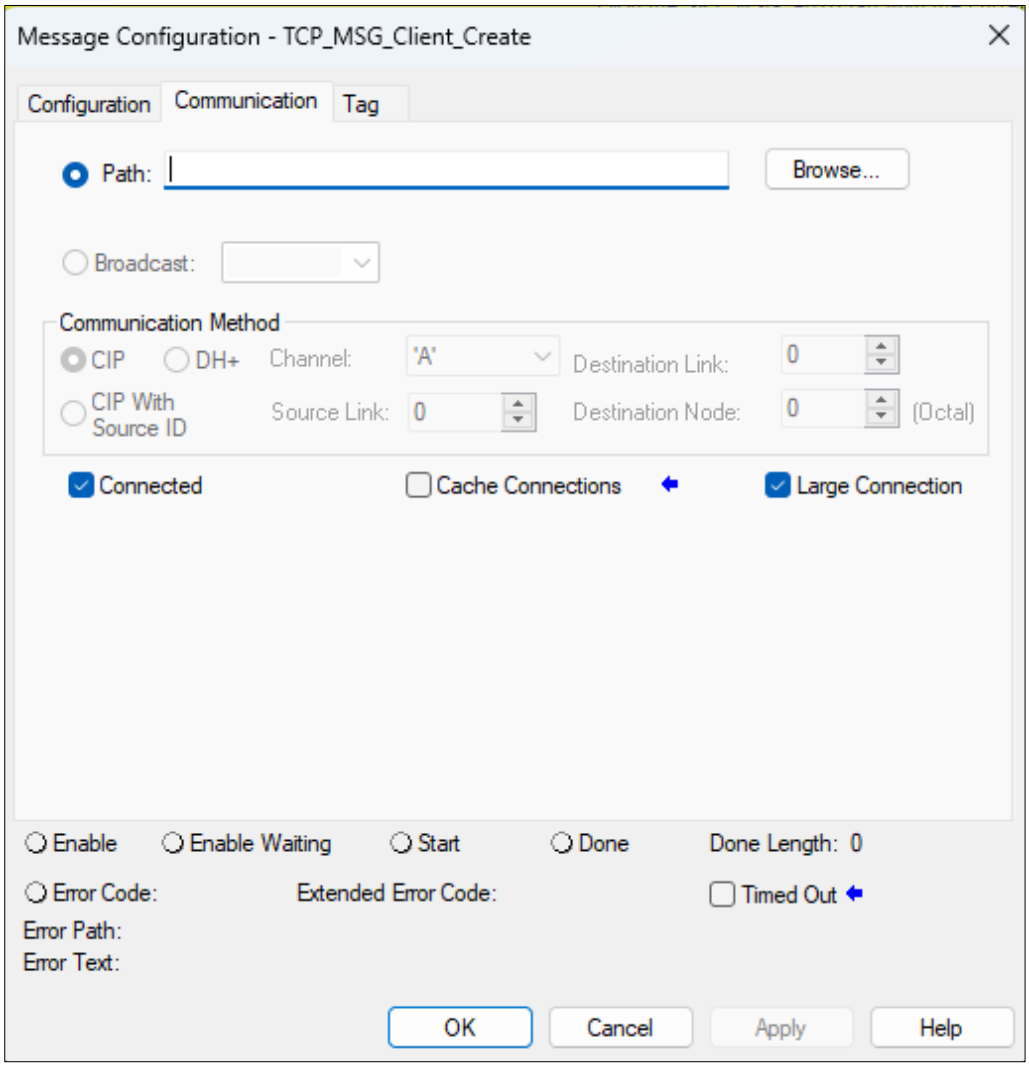

Message Configuration - TCP_MSG_Client_Create
Configuration
Communication
Tag
Path:
Browse...
Broadcast:
Communication Method
CIP
DH+
Channel:
'A'
Destination Link:
0
CIP With Source ID
Source Link:
0
Destination Node:
0
(Octal)
Connected
Cache Connections
Large Connection
Enable
Enable Waiting
Start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

Bild 43

7.3.2.4 Konfiguration des “Read_MSG”-Befehls

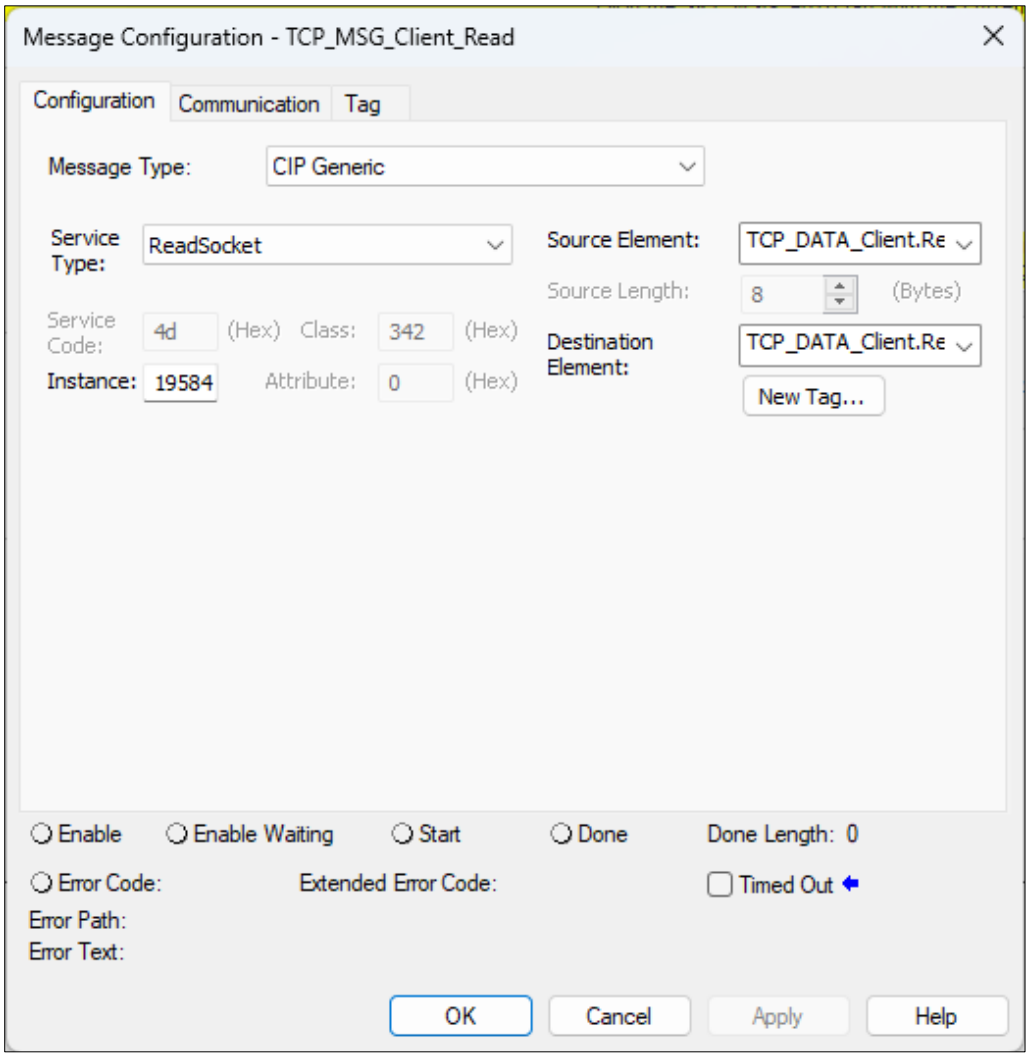


Bild 44

7.3.2.5 Konfiguration des “Write_MSG”-Befehls

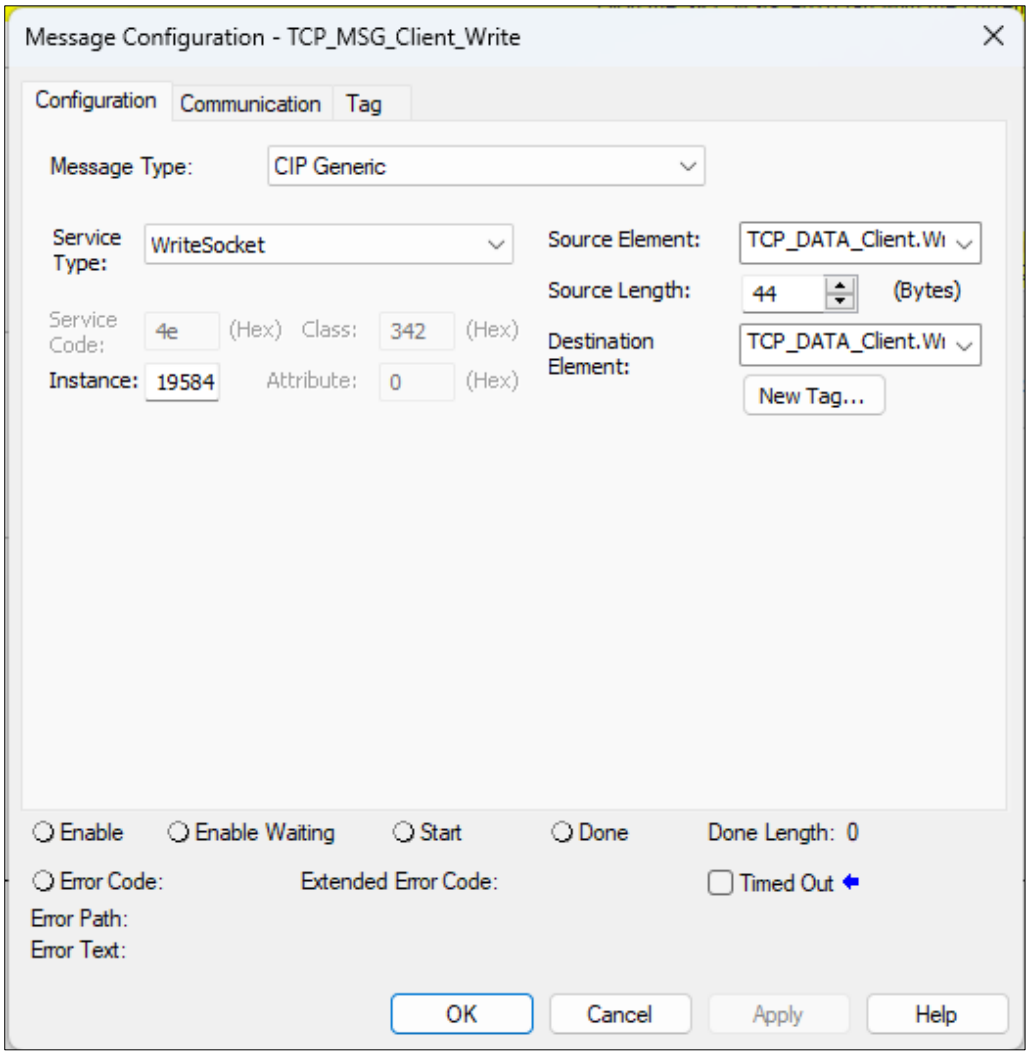


Bild 45

7.3.2.6 Konfiguration des “Delete_MSG”-Befehls

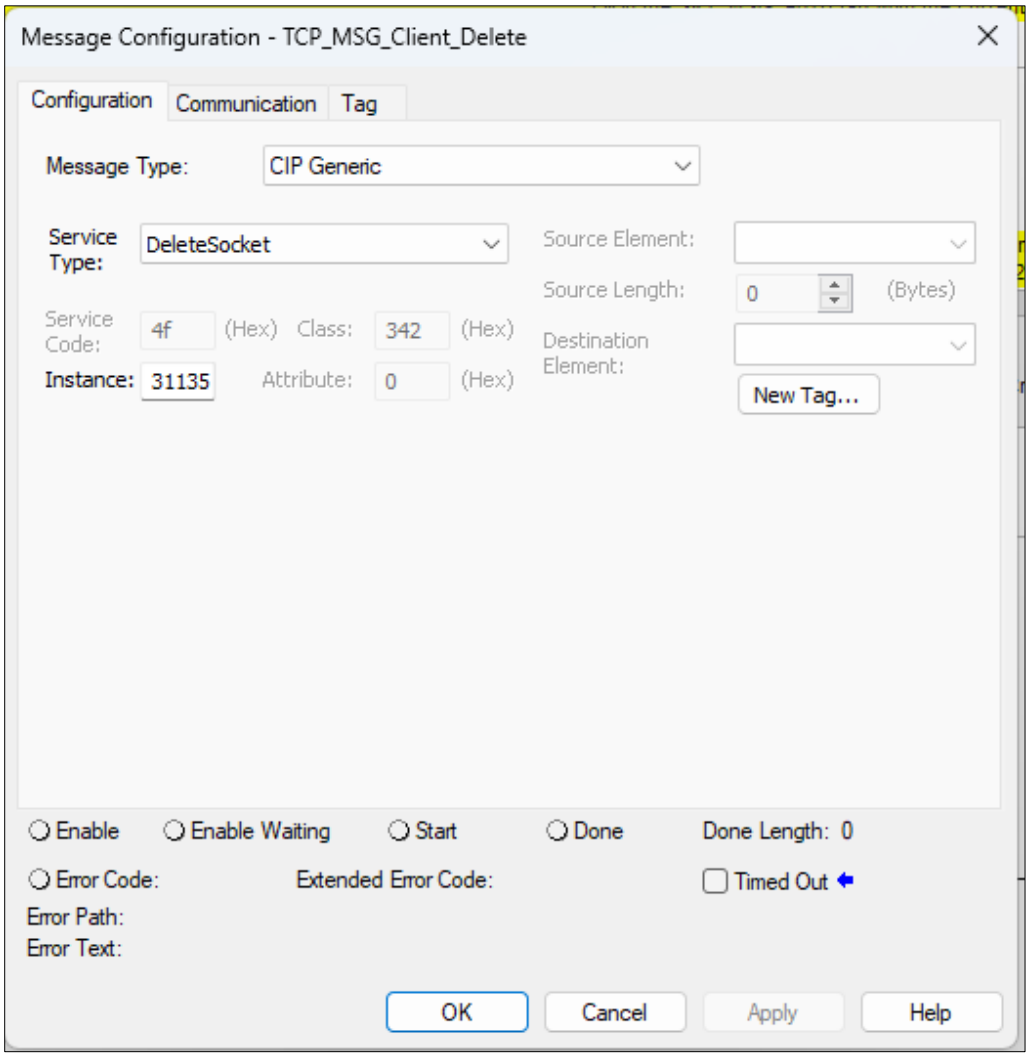


Bild 46

7.3.3 Konfiguration der Temperatursensors und Receiver

Nach Beendigung der beschriebenen Schritte aus der kompletten oder manuellen Installation kann nun die abschließende Konfiguration der verwendeten Temperatursensoren vorgenommen werden.
Dafür wurde ein Tag namens „BLE1_Parameter“ mit Datentyp „udt_VBLE_TempSens_Parameters“ im lokalen Programm erstellt, der folgendermaßen aussieht:

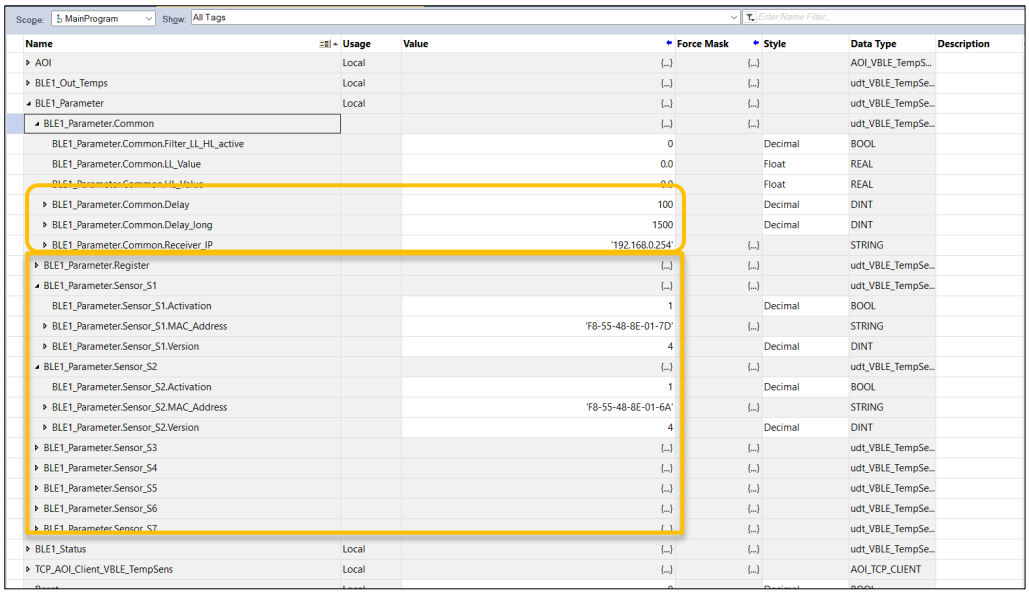


Bild 47

Innerhalb dieser Tags kann die Konfiguration der verwendeten Receiver-Schnittstelle und der Temperatur-Sensoren eingegeben werden.
Die Receiver-Schnittstelle benötigt nur die verwendete IP der Schnittstelle unter „Common.Receiver_IP“.

Es ist wichtig die Tags “Delay“ und „Delay_long“, wie in den nachfolgenden Bildern gezeigt, anzupassen. So wird die Funktion sichergestellt.

Für jeden Temperatur-Sensor (Sensor 1 bis maximal Sensor 7) muss die MAC-Adresse, welche auf dem jeweiligen Sensor im Format XX-XX-XX-XX-XX-XX graviert ist sowie die Version des Sensor eingegeben werden.

7.3.4 Empfang Temperatur-Ergebnisse von Tags

Nach Beendigung der Installation und Starten der Temperaturmessung durch Verwendung des Tags „Enable“ aus dem Befehl findet die Kommunikation mit dem Receiver statt. Die aktuellen Temperaturen (Tip- und Board-Temperatur) werden in Echtzeit ausgelesen und sortiert nach Sensoren im Tag „BLE1_Out_Temps“ zur weiteren Verwendung platziert.

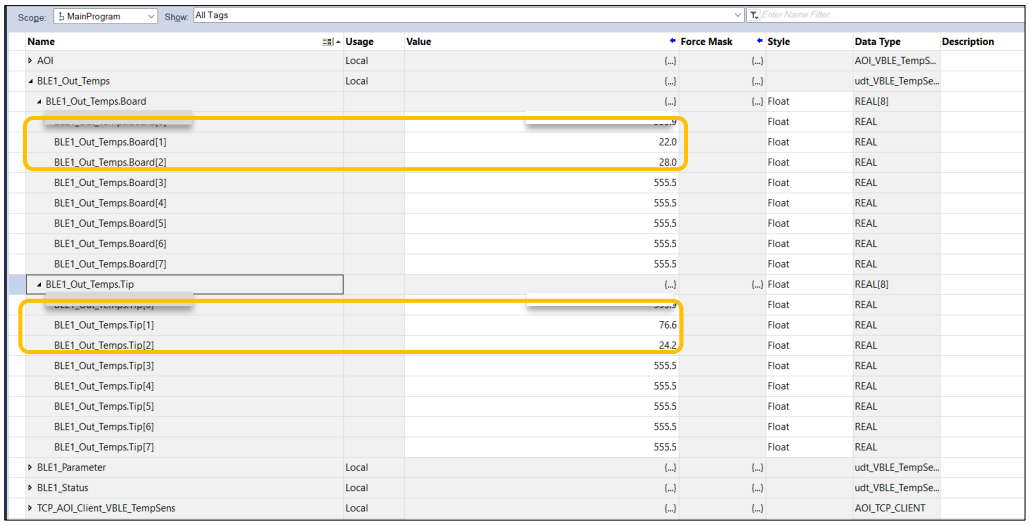


Bild 48

7.3.5 Beispiel-Visualisierung mit “FT View Studio”

Einrichten der Sensor-MAC-Adressen

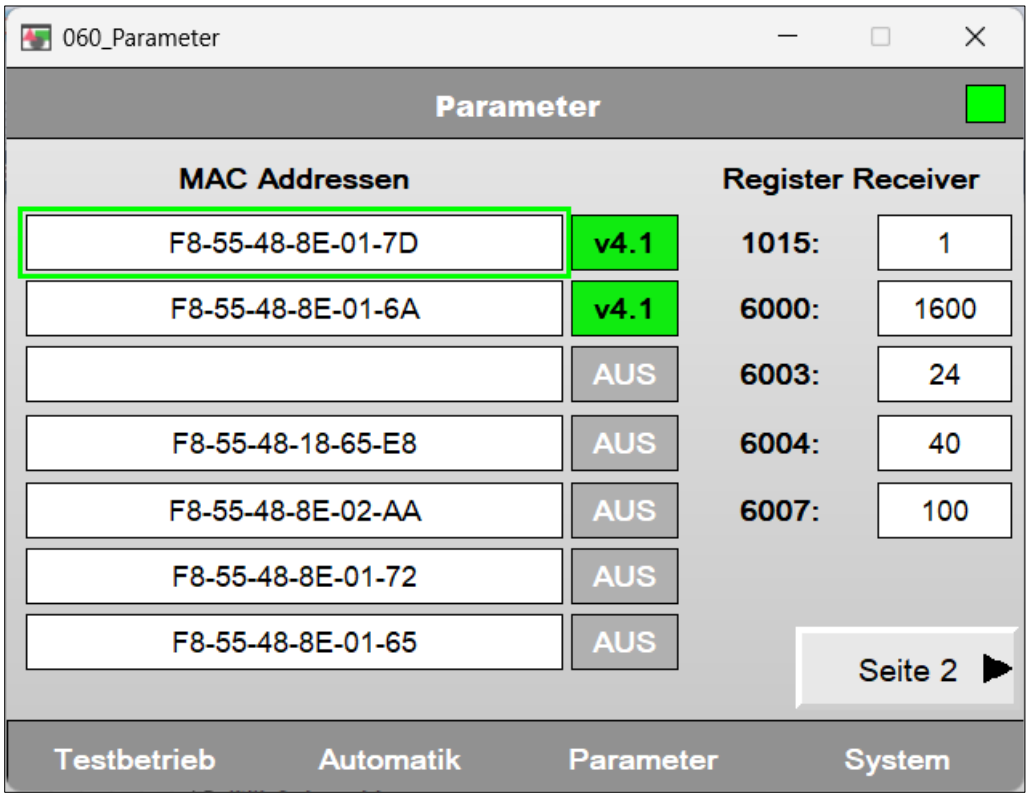


Bild 49

Einrichten der Receiver-IP-Adresse

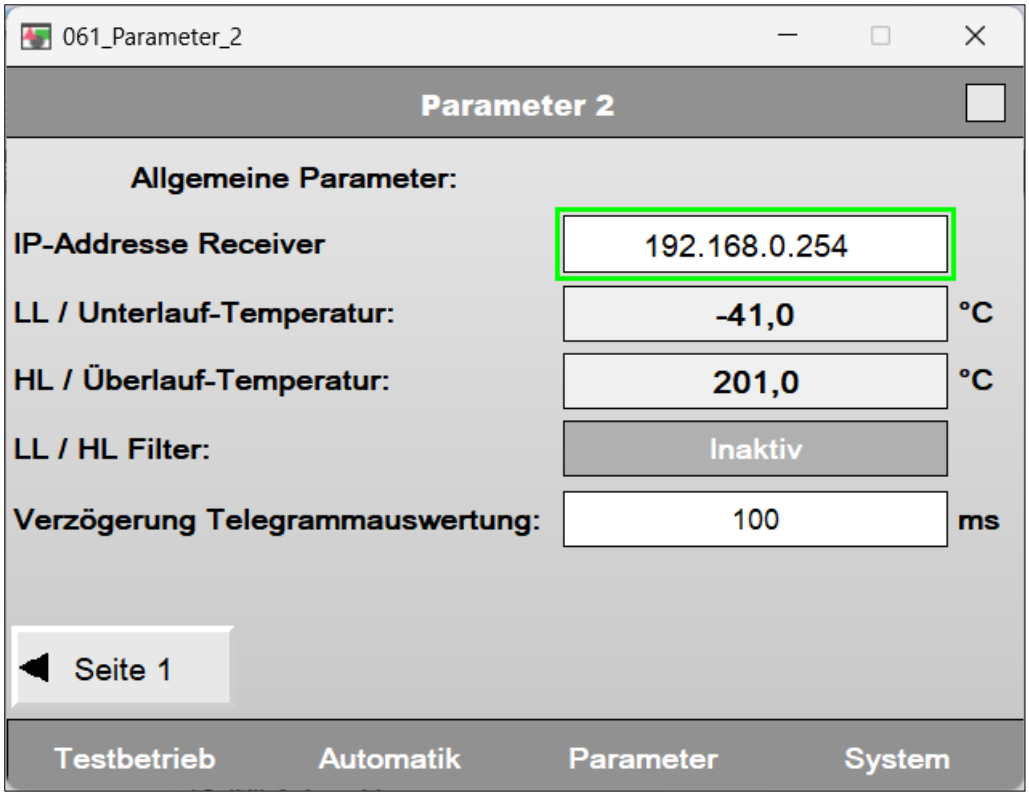


Bild 50

Start Messung

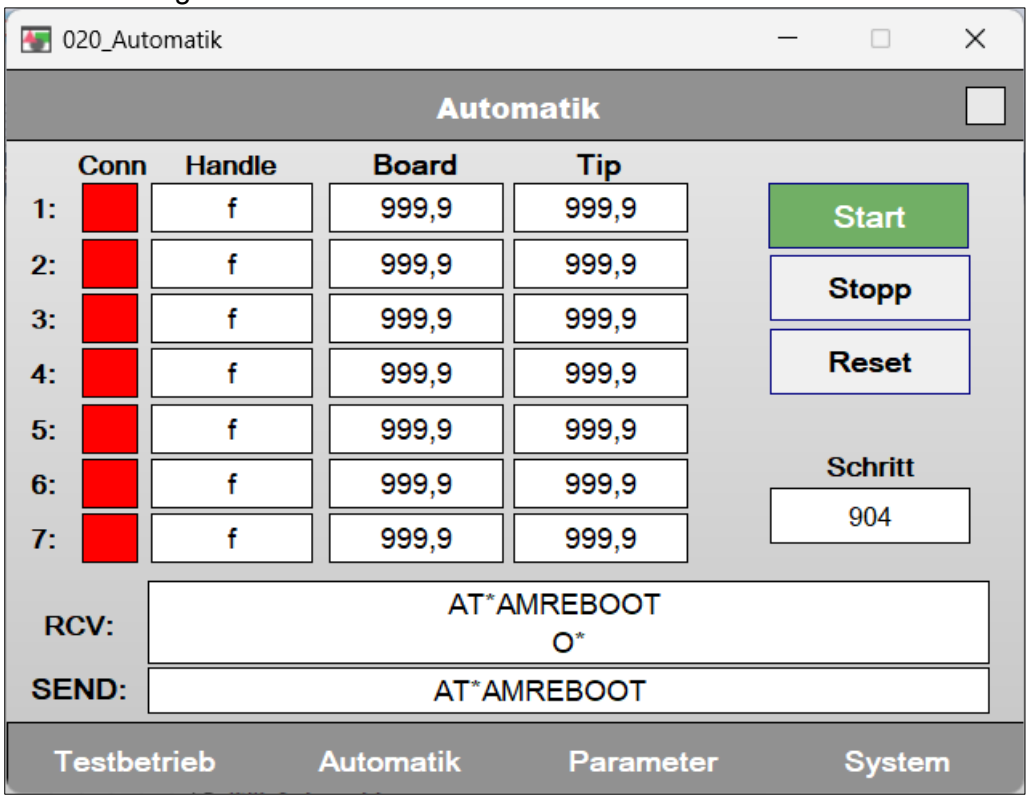


Bild 51

Die Messung ist gestartet und die Temperaturwerte werden angezeigt

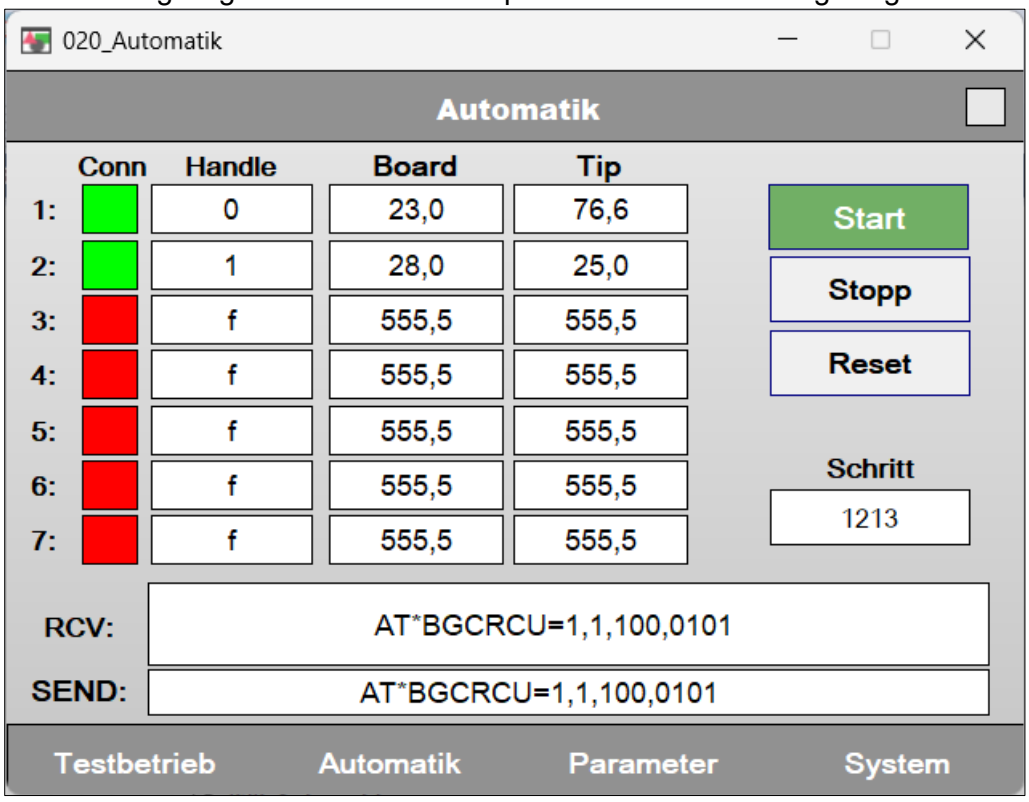


Bild 52

7.3.6 Anlage

7.3.6.1 Startvorrausetzung

Folgenden Voraussetzungen müssen erfüllt sein, damit der Automatikbetrieb erfolgen kann:

- Mindestens 1 Sensor aktiviert
- Kein Firewall zwischen CPU und Receiver
- 100 Meter pro Segment ist die maximale Länge des LAN-Kabels
- Das LAN-Kabel muss geschirmt sein und mindestens Cat5 (100 Mbit/s) entsprechen
- Kein Fehler bei der Eingabe der MAC-Adressen
- Keine Störung aktiv

8 Inbetriebnahme

⚠ WARNUNG

Verletzungsgefahr
Beachten Sie bei Arbeiten an der Berührungslosen Thermischen Messeinrichtung (OnSens.SmarTemp) insbesondere → Kapitel 5 (Sicherheit)!

- Eine nicht fachgerecht ausgeführte Inbetriebnahme könnte Personen-, Sach-, oder Umweltschäden verursachen!
- Die Durchführung der Inbetriebnahme, insbesondere das erstmalige Starten der Turbokupplung darf nur durch Fachkräfte erfolgen!
- Sichern Sie die Anlage gegen unbefugtes Einschalten!
- Der Receiver benötigt nach Anschließen an die Spannungsversorgung eine Initialisierungszeit von **ca. 10 s**, erst danach ist das OnSens.SmarTemp betriebsbereit und die Turbokupplung darf gestartet werden.

- Verdrahtung überprüfen. Achten Sie insbesondere auf die richtige Verdrahtung der Versorgungsspannung!
- Versorgungsspannung an dem Receiver anlegen.
- Der Receiver benötigt eine Initialisierungszeit von ca. 10 s.
- Der reguläre Betrieb kann aufgenommen werden. Bei Störungen, → Kapitel 11.
- Nach Start der Turbokupplungen benötigt der Temperaturfühler einen gewissen Zeitraum, um die benötigte interne Spannung zu erzeugen. Falls die Temperatur des Betriebsmediums bereits mehr als ca. 20 Kelvin höher als die Umgebungstemperatur ist beträgt dieser Zeitraum mehrere Sekunden, bis das erste Temperatursignal gesendet wird. Falls das Betriebsmedium der Turbokupplung weniger als ca. 20 Kelvin im Verhältnis zur Umgebung erwärmt ist (z. B. längerer Stillstand, Leerlaufbetrieb, Betrieb mit niedriger Last) reicht die interne Spannungsversorgung nicht aus und der Temperaturfühler sendet kein bzw. kein stabiles kontinuierliches Signal. Erst nach Überschreitung der benötigten Temperaturdifferenz von ca. 20 Kelvin im stationären Zustand startet der Temperaturfühler mit der stabilen Signalübertragung ohne Unterbrechungen. Im instationär erwärmten Zustand des Temperaturfühlers (z. B. Maschinenanlauf) beträgt die benötigte Temperaturdifferenz bis zu 60 Kelvin. Eine entsprechende Überbrückung muss in der Maschinensteuerung realisiert werden.

9 Wartung, Instandhaltung

Wartung und Instandhaltung: Eine Kombination aller Tätigkeiten, die ausgeführt werden, um einen Gegenstand in einem Zustand zu erhalten oder ihn wieder dahin zu bringen, der den Anforderungen der betreffenden Spezifikation entspricht und die Ausführung der geforderten Funktionen sicherstellt.

Inspektion: Eine Tätigkeit, die die sorgfältige Untersuchung eines Gegenstandes zum Inhalt hat, mit dem Ziel einer verlässlichen Aussage über den Zustand dieses Gegenstandes, wobei sie ohne Demontage oder, falls erforderlich, mit teilweiser Demontage, ergänzt durch Maßnahmen, wie z.B. Messungen durchgeführt wird.

Sichtprüfung: Eine Sichtprüfung ist eine Prüfung, bei der ohne Anwendung von Zugangseinrichtungen oder Werkzeugen sichtbare Fehler festgestellt werden, z.B. fehlende Schrauben.

Nahprüfung: Eine Prüfung, bei der zusätzlich zu den Aspekten der Sichtprüfung solche Fehler festgestellt werden, wie z.B. lockere Schrauben, die nur durch Verwendung von Zugangseinrichtungen, z.B. mobile Treppenstufen (falls erforderlich), und Werkzeugen zu erkennen sind. Für Nahprüfungen braucht ein Gehäuse üblicherweise nicht geöffnet oder die Betriebsmittel spannungsfrei geschaltet zu werden.

Detailprüfung: Eine Prüfung, bei der zusätzlich zu den Aspekten der Nahprüfung solche Fehler festgestellt werden, wie z.B. lockere Anschlüsse, die nur durch das Öffnen von Gehäusen und/oder, falls erforderlich durch Verwendung von Werkzeugen und Prüfeinrichtungen zu erkennen sind.

⚠ WARNUNG

Verletzungsgefahr
Beachten Sie bei Arbeiten an der Berührungslosen Thermischen Messeinrichtung (OnSens.SmarTemp) insbesondere → Kapitel 5 (Sicherheit)!
- Halten Sie stets die Zugangswege zur Turbokupplung frei!

Qualifikation
→ Kapitel 5.8

- Nur qualifizierte und berechtigte Fachkräfte dürfen Instandhaltungs- und Wartungsarbeiten durchführen! Die Qualifikation wird durch Schulung und Einweisung an der Turbokupplung sichergestellt.
- Folgen einer nicht fachgerechten Instandhaltung und Wartung könnten Tod, schwere oder leichte Verletzungen, Sachschäden oder Umweltschäden sein.

- Schalten Sie die Anlage, in die die Turbokupplung eingebaut ist aus und sichern Sie den Schalter gegen Wiedereinschalten.
- Stellen Sie bei allen Arbeiten an der Turbokupplung sicher, dass sich sowohl der Antriebsmotor als auch die Arbeitsmaschine im Stillstand befinden und ein Anlaufen unter allen Umständen ausgeschlossen werden kann!
- Der Austausch von Komponenten darf nur mit Original-Ersatzteilen erfolgen.

Unmittelbar nach Abschluss der Instandhaltungs- und Wartungsarbeiten montieren Sie wieder alle Schutzverkleidungen und Sicherheitseinrichtungen in der ursprünglichen Lage. Überprüfen Sie deren einwandfreie Funktion!

Wartungsplan:

Termin	Wartungsarbeiten
Spätestens 3 Monate nach Inbetriebnahme, dann jeweils jährlich	Anlage auf Unregelmäßigkeiten hin inspizieren (Sichtprüfung).
	Prüfen der elektrischen Anlage auf Unversehrtheit (Detailprüfung).
Bei Verunreinigung	Reinigung (→ Kapitel 9.1).

Tabelle 7

- Wartungsarbeiten und laufende Prüfungen sind entsprechend Protokoll vorzunehmen.
- Wartungsarbeiten protokollieren.

Protokollvorlagen → Betriebsanleitung der Turbokupplung

9.1 Außenreinigung

HINWEIS

Sachschaden
Beschädigung des OnSens.SmarTemp durch unsachgemäße, ungeeignete Außenreinigung.
- Achten Sie auf die Verträglichkeit des Reinigungsmittels mit der Vergussmasse des OnSens.SmarTemp.
- Verwenden Sie kein Hochdruckreinigungsgerät!
- Gehen Sie vorsichtig mit Dichtungen um. Vermeiden Sie Wasser- und Druckluftstrahl.

- OnSens.SmarTemp nach Bedarf mit einem fettlösenden Mittel reinigen.

10 Entsorgung

Entsorgen der Verpackung
Entsorgen Sie das Verpackungsmaterial gemäß den örtlichen Vorschriften.

Entsorgen von Betriebsflüssigkeiten
Beachten Sie bei der Entsorgung die entsprechenden Gesetze sowie Angaben des Herstellers bzw. Lieferanten.

Entsorgen des OnSens.SmarTemp
Entsorgen Sie das OnSens.SmarTemp gemäß den örtlichen Vorschriften.

Entnehmen Sie spezielle Hinweise zur Entsorgung von verwendeten Stoffen und Materialien der folgenden Tabelle:

	Entsorgungsart		
Material / Stoff	**Wiederverwertung**	**Restmüll**	**Sondermüll**
Metalle	x	-	-
Kabel	x	-	-
Dichtungen	-	x	-
Kunststoffe	x [1)]	(x)	-
Betriebsmittel	-	-	x [1), 2)]
Verpackung	x	-	-

Tabelle 8

1) falls möglich
2) nach Sicherheitsdatenblatt oder Herstellerangaben entsorgen

11 Störungen – Abhilfe, Fehlersuche

⚠ WARNUNG

Verletzungsgefahr
Beachten Sie bei Arbeiten an der Berührungslosen Thermischen Messeinrichtung (OnSens.SmarTemp) insbesondere → Kapitel 5 (Sicherheit)!

Die nachstehende Tabelle soll Ihnen helfen, bei Betriebsstörungen schnell die Ursache zu ermitteln und evtl. Abhilfe zu schaffen.

Betriebsstörung	mögliche Ursache(n)	Abhilfe	siehe
Der Receiver hat keine Anzeige (LED „PWR“ leuchtet nicht).	Fehlende, falsche oder verpolte Spannungsversorgung.	Spannungsversorgung und Verdrahtung prüfen. Spannungsversorgung korrekt anlegen.	Kapitel 6.4
	Der Receiver ist defekt.	Receiver austauschen.	

Betriebsstörung	mögliche Ursache(n)	Abhilfe	siehe
Maschinensteuerung empfängt kein Temperatursignal (bzw. Temperatursignal 999,9°C)	Datenkabel zwischen Receiver und Maschinensteuerung nicht korrekt angeschlossen (LED „LAN“ leuchtet nicht)	Verdrahtung Datenkabel zur übergeordneten Steuerung überprüfen.	
	Receiver nicht korrekt in die Maschinensteuerung eingebunden.	Implementierung überprüfen.	Kapitel 7
	Falsche Sensor-MAC-Adresse in die Maschinensteuerung hinterlegt.	MAC-Adresse (Gravur auf Sensor) mit Eingabe vergleichen und korrigieren	Kapitel 7.2
	Temperatur des Betriebsmedium der Turbokupplung geringer als 20 Kelvin über Umgebungstemperatur	Temperatur Betriebsmedium erhöhen durch z.B. Erhöhung der Lastaufnahme der Arbeitsmaschine.	Kapitel 2.1
	Reichweite Signal, Abstand zwischen Temperaturfühler und Receiver zu groß	Montage des Receivers in Reichweite zum Temperaturfühler. Abschirmungen (z.B. geschlossener Schaltschrank) vermeiden	Kapitel 6.4
	Temperaturfühler ist defekt.	Temperaturfühler auf Beschädigungen prüfen, ggf. Temperaturfühler austauschen.	
Maschinensteuerung empfängt nur sporadisch kein Temperatursignal (bzw. Temperatursignal 999,9°C)	Temperatur des Betriebsmedium der Turbokupplung leicht geringer oder nahe der 20 Kelvin über Umgebungstemperatur	Temperatur Betriebsmedium erhöhen durch z.B. Erhöhung der Lastaufnahme der Arbeitsmaschine.	Kapitel 2.1
Ausgegebene Temperatur falsch.	Receiver nicht korrekt in die Maschinensteuerung eingebunden.	Implementierung überprüfen.	Kapitel 7
	Temperaturfühler ist defekt.	Temperaturfühler auf Beschädigungen prüfen, ggf. Temperaturfühler austauschen.	

Betriebsstörung	mögliche Ursache(n)	Abhilfe	siehe
Undichtigkeit an der Turbokupplung	Undichtigkeit an der Verschraubung Temperaturfühler oder OnSens.SmarTemp-Blindschraube	Korrekter Sitz Dichtring kontrollieren, Anzugsmoment kontrollieren	Kapitel 6.2 und 6.3
Betriebsmediumsverlust über die Schmelz-sicherungsschrauben.	Anlagenüberwachung ist nicht korrekt auf die Ansprechtemperatur oder Schmelz-sicherungsschrauben (FP) abgestimmt, Temperaturfehler des OnSens.SmarTemp nicht korrekt berücksichtigt.	Temperaturüber-wachung der Anlagensteuerung prüfen. Temperaturfehler des OnSens.SmarTemp korrekt berücksichtigen. Halten Sie ggf. Rücksprache mit Voith.	Kapitel 3.1
	Temperatur der Voith Turbokupplung (VTK) beim Motorstart ist zu hoch.	Abkühlzeit beachten, ggf. Temperatur vor dem Motorstart händisch messen.	
	Überlast, die bei der Auslegung der VTK nicht berücksichtigt wurde.	Bestimmungsgemäßen Betrieb sicherstellen, unzulässige Überlast vermeiden.	
	Lastrücknahme bei Übertemperatur zu gering oder zu spät.	Reaktion der Anlage auf Laständerungen ermitteln. Lastrücknahme optimieren (Bediener/Software).	
	Abschaltung bei Übertemperatur erfolgt zu spät.	Reaktion der Anlage auf Abschaltung ermitteln. Abschaltung optimieren (Bediener/Software).	
	Ausgegebene Temperatur ist zu niedrig.	Siehe Betriebsstörung “Ausgegebene Temperatur falsch“.	
Halten Sie bitte Rücksprache mit Voith (→ Kapitel 12), falls eine Betriebsstörung auftreten sollte, die nicht in dieser Tabelle erfasst ist.			

Tabelle 9

12 Rückfragen, Monteur- und Ersatzteilbestellung

Bei

- Rückfragen
- Monteurbestellung
- Ersatzteilbestellung
- Inbetriebnahmen

benötigen wir:

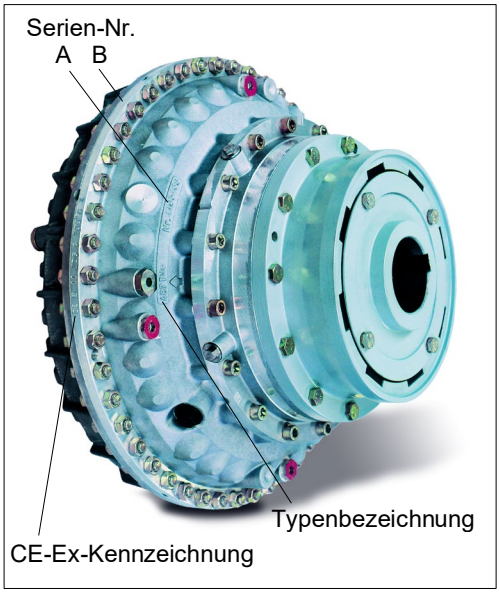


Bild 53

die **Serien-Nr.** und **Typenbezeichnung** der Turbokupplung an der das OnSens.SmarTemp eingesetzt wird.

→ die Serien-Nr. und Typenbezeichnung finden Sie entweder am Außenrad / Kupplungsschale (A) oder am Umfang (B) der Turbokupplung.

→ Die Serien-Nr. ist mit Schlagzahlen eingeschlagen.

→ Turbokupplungen, die für den Einsatz im explosionsgefährdeten Bereich bestimmt sind, finden Sie die CE-Ex-Kennzeichnung am Umfang der Turbokupplung.

Bei einer **Monteurbestellung,** einer **Inbetriebnahme** oder einem **Service** benötigen wir zusätzlich

- den Aufstellungsort der Turbokupplung,
- einen Ansprechpartner und dessen Adresse,
- eine Beschreibung der aufgetretenen Störung.

Kontakt
→ Seite 2

Bei einer **Ersatzteilbestellung** benötigen wir zusätzlich

- die Versandadresse für die Ersatzteillieferung.

13 Ersatzteilinformation

HINWEIS

Nehmen Sie keine eigenmächtigen Änderungen und Nachrüstungen vor!
Führen Sie keine Nachrüstungen mit Ausrüstungsteilen oder Betriebsmitteln anderer Hersteller durch!
Veränderungen oder Umbauten ohne die vorherige schriftliche Zustimmung der Firma Voith haben den Verlust jeglicher Gewährleistung zur Folge! Generelle Ansprüche verfallen!

- Eine fachmännische Instandsetzung bzw. Reparatur kann nur durch den Hersteller gewährleistet werden!

13.1 Temperaturfühler

Temperaturfühler			Dichtring
Verwendung für Turbokupplungsgröße	**Gewinde-abmessung**	**Material-Nr.**	**Material-Nr.**
366 - 650	M18x1,5	201.04653810	TCR.03658018
750 - 1330	M24x1,5	201.04653910	H01.105249

Tabelle 10

13.2 OnSens.SmarTemp -Blindschrauben

Blindschraube			Dichtring
Verwendung für Turbokupplungsgröße	**Gewinde-abmessung**	**Material-Nr.**	**Material-Nr.**
366 - 650	M18x1,5	201.04461010	TCR.03658018
750 - 1330	M24x1,5	201.04461110	H01.105249

Tabelle 11

13.3 Stationärer Receiver

Verwendung für Turbokupplungsgröße	Material-Nr.
366 – 1330	201.04641410

Tabelle 12

13.3.1 Kabel Spannungsversorgung 5 Meter

Verwendung für Turbokupplungsgröße	Material-Nr.
366 – 1330	201.04460210

Tabelle 13

13.3.2 Kabel Netzwerk 5 Meter

Verwendung für Turbokupplungsgröße	Material-Nr.
366 – 1330	201.04460310

Tabelle 14

14 Anhang

EU Konformitätserklärung

Hersteller:	J.M. Voith SE & Co. KG Voithstraße 1 74564 Crailsheim, DEUTSCHLAND
Bezeichnung:	**Berührungslose thermische Messeinrichtung**
Typ:	**OnSens.SmarTemp**

Die berührungslose thermische Messeinrichtung besteht aus:

- OnSens.SmarTemp-Sensor (Temperaturfühler)
- OnSens.SmarTemp Blindschraube
- Stationärer Receiver

Die alleinige Verantwortung für die Ausstellung dieser Konformitätserklärung trägt der Hersteller.

Die oben beschriebene berührungslose thermische Messeinrichtung entspricht den folgenden einschlägigen Harmonisierungsrechtsvorschriften der Union:

- 2014/53/EU (Richtlinie über Funkanlagen) / 22.5.2014 | DE | Amtsblatt der Europäischen Union | L 153/62
- 2011/65/EU (RoHS Richtlinie) / 08.6.2011 | DE | Amtsblattmitteilung der Europäischen Union | L 174/88

Folgende harmonisierte Normen (oder Teile hieraus) wurden angewandt:

- EN 300 328 V2.2.2

Weitere angewandte Normen und technische Spezifikationen:

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

Unterzeichnet für und im Namen von J.M. Voith SE & Co. KG:

Berroth, Hannes

Digital unterschrieben von Berroth, Hannes
Datum: 2026.05.12 09:15:58 +02'00'

Crailsheim	11.05.2026	Hannes Berroth (Vice President CCE HDC)
Ort	**Datum**	**Name, Position, Unterschrift**

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
1.1. About This Document 1
1.2. Document Conventions 1
1.3. Trademarks 2

2. Safety 3
2.1. General Safety 3
2.2. External Antenna Restrictions 3
2.3. Intended Use 3

3. Cybersecurity 4
3.1. General Cybersecurity 4
3.2. Security Advisories 5
3.3. How to Report a Vulnerability 5
3.4. Product Cybersecurity Context 6
3.4.1. Bridge II Ethernet Interfaces 6
3.4.2. Services 7

4. Preparation 8
4.1. Support and Resources 8
4.2. Optional Equipment 8
4.3. Network Environment 8
4.4. Placement for Optimal Reception 8
4.5. When to Use Bluetooth or WLAN 9
4.6. Bluetooth Limitations 9
4.7. I/O-Data Cycle Time Considerations 9

5. Installation 10
5.1. Installation Drawing 10
5.2. Surface Mounting 11
5.3. DIN Rail Mounting 12
5.4. Connect to LAN and Power 13

6. Configuration 15
6.1. Bridge II Ethernet Built-In Web Interface 15
6.2. Connect to Configure 16
6.3. Access the Built-In Web Interface 17
6.3.1. Required IP Address Settings 17
6.3.2. Login to the Built-In Web Interface 19
6.4. To Save and Reboot 20
6.5. Factory Default Settings 21
6.6. Configuration Methods 21
6.7. Configuration with Easy Config 22
6.7.1. Available Easy Config Modes 22
6.7.2. Easy Config Modes Time Considerations 23
6.7.3. Easy Config Using the MODE Button 24
6.7.4. Easy Config Using the Built-In Web Interface 28
6.8. Configuration with AT Commands 31
6.8.1. Enable Fast Roaming with AT Commands 32
6.8.2. Add Additional WLAN Channels with AT Commands 33
6.8.3. To Use Bluetooth LE With AT Commands 34
6.9. Configure Settings in the Built-In Web Interface 35

6.9.1. Network Settings 35
6.9.2. Traffic Control 37
6.9.3. Layer 3 IP Forward Connectivity Considerations 38
6.9.4. WLAN Settings General 39
6.9.5. WLAN Settings for Client 39
6.9.6. WLAN Roaming 39
6.9.7. WLAN Channels and World Mode 40
6.9.8. WLAN Settings for Access Point 41
6.9.9. WLAN Advanced Settings 43
6.9.10. Bluetooth Settings General 44
6.9.11. Bluetooth Settings for PANU Mode 45
6.9.12. Bluetooth Settings for NAP Mode 46
6.9.13. Bluetooth LE Settings 47
6.9.14. System Settings 48

7. Verify Operation 51
7.1. LED Indicators 51
7.2. Network Connection Status 53

8. Use Cases 54
8.1. Easy Config Using MODE Button: Confirm Connection Example 54
8.2. Ethernet Bridge via WLAN or Bluetooth 57
8.3. PROFINET Networking Via Bluetooth 59
8.4. EtherNet/IP Networking Via Bluetooth 61
8.5. Ethernet Network to Existing WLAN 63
8.6. Adding Single Ethernet Node to WLAN 65
8.7. Access PLC from Handheld Device via WLAN 66

9. Maintenance 68
9.1. Manually Update Firmware 68
9.2. Automatically Check for Firmware Updates 70
9.3. Automatically Update Firmware 71
9.4. Settings Backup 72
9.4.1. Create Settings Backup File 72
9.4.2. Restore Settings From Backup File 73

10. Troubleshooting 74
10.1. Recovery Mode 74
10.2. Reset to Factory Default 75

11. End Product Life Cycle 77
11.1. Secure Data Disposal 77

12. Technical Data 78
12.1. Technical Specifications 78

13. Reference Guides 80
13.1. Wireless Technology Basics 80
13.2. Internal Antenna Characteristics 81
13.2.1. Internal Antenna Positions 81
13.2.2. Lab Environment Diagrams 82
13.2.3. Real World Measurements 84

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

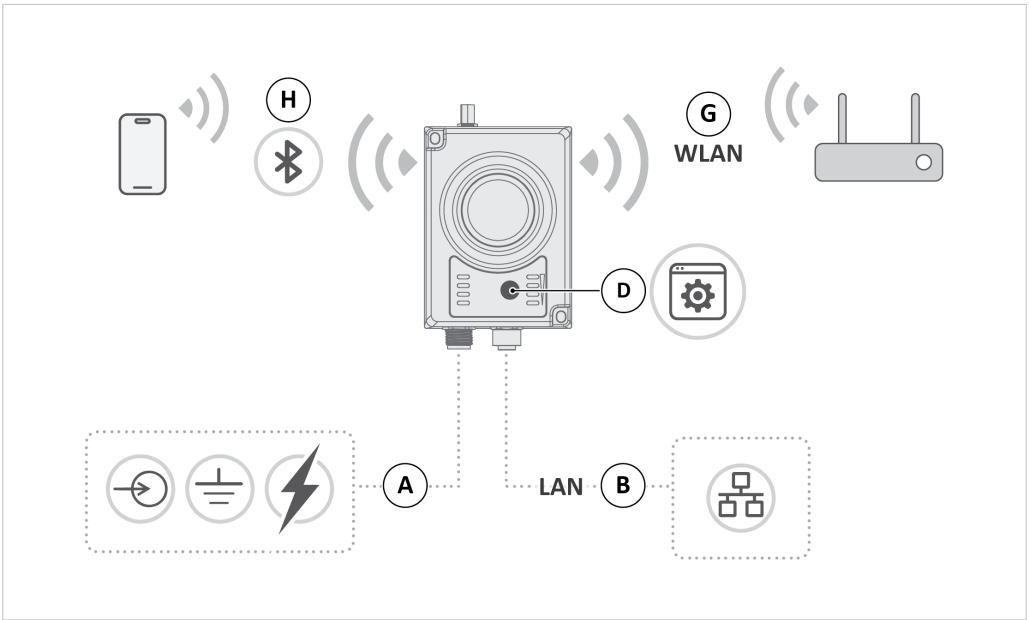


Figure 1. Bridge II Ethernet interfaces

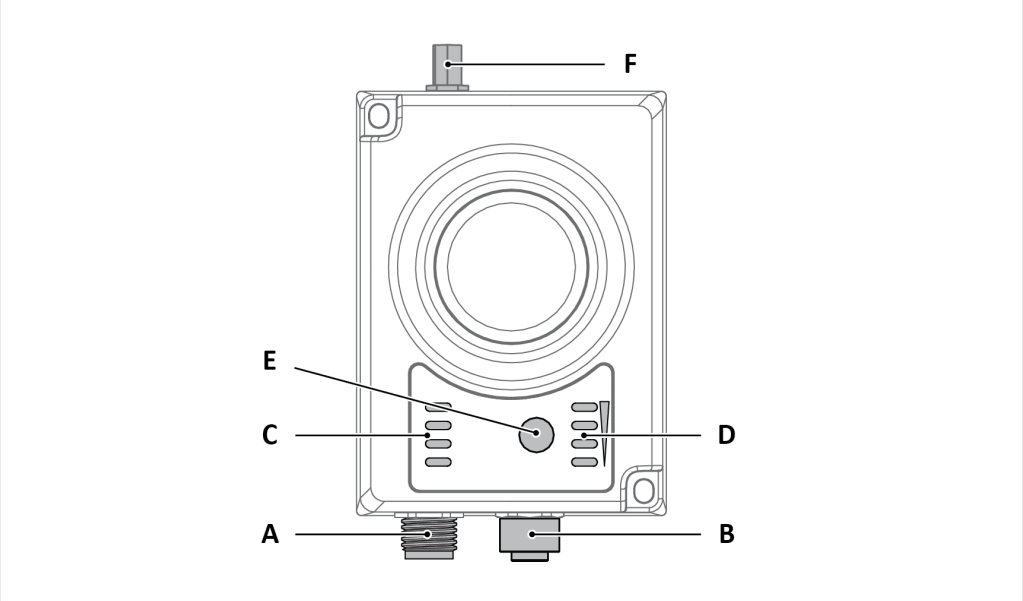


Figure 2. Bridge II Ethernet External parts

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.

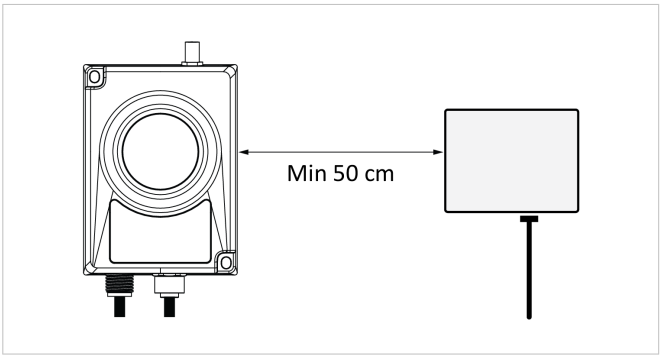


Figure 3. Required minimum distance between wireless devices

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.

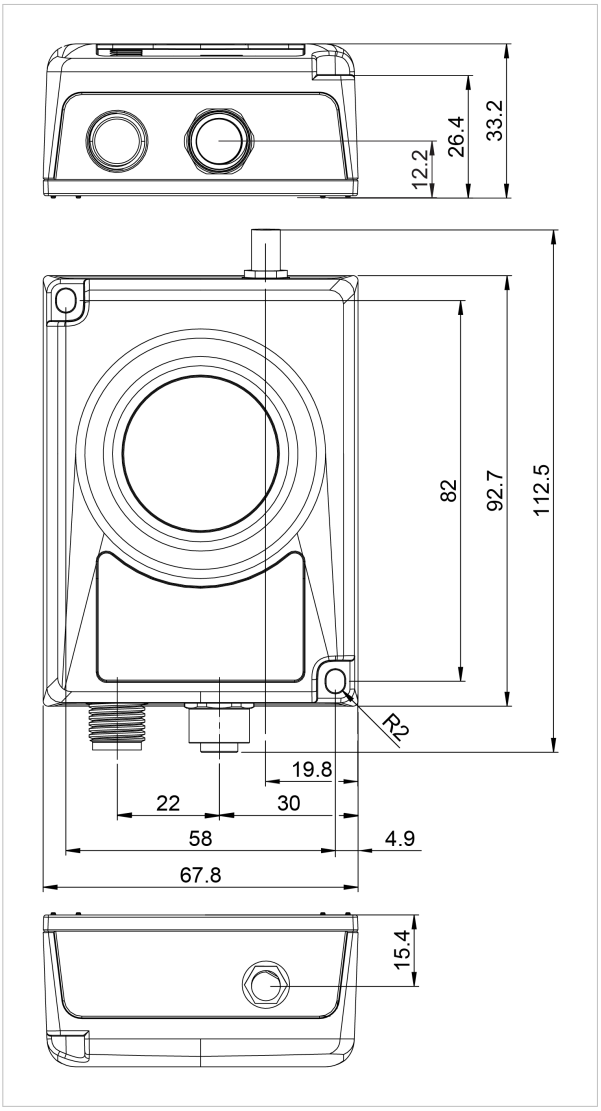
4.7. I/O-Data Cycle Time Considerations

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

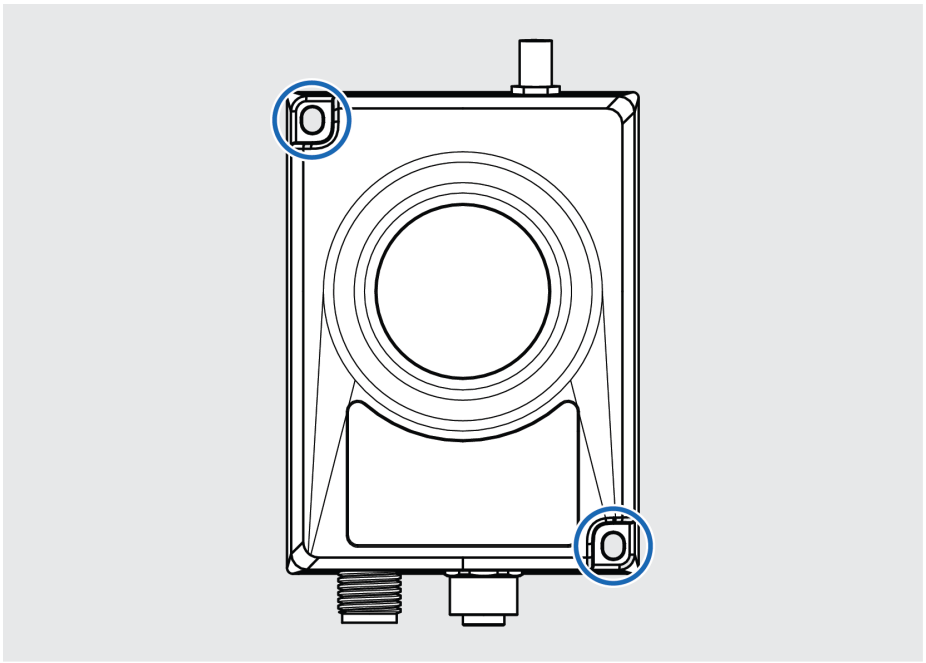


Figure 5. Surface mounting holes

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.

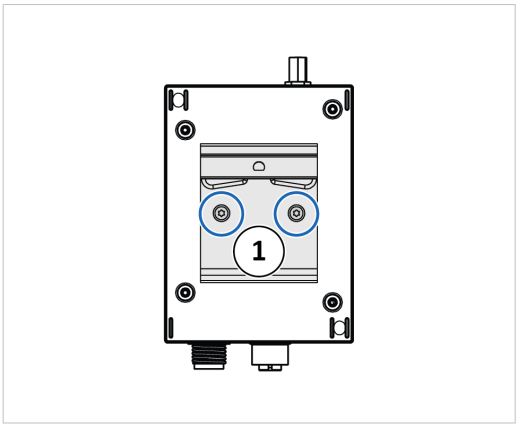


Figure 6. DIN clip on Bridge II Ethernet

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.

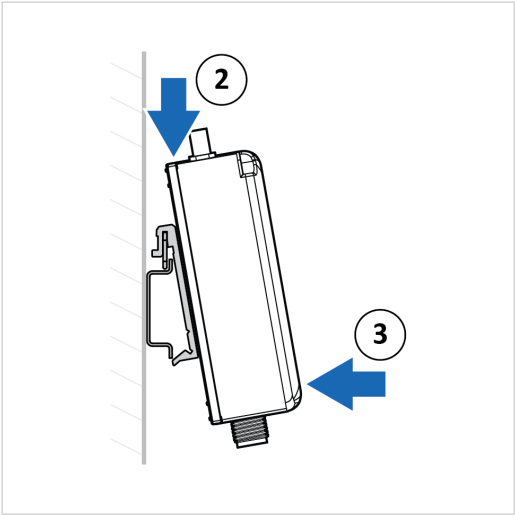


Figure 7. Attach Bridge II Etherneton DIN rail

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.

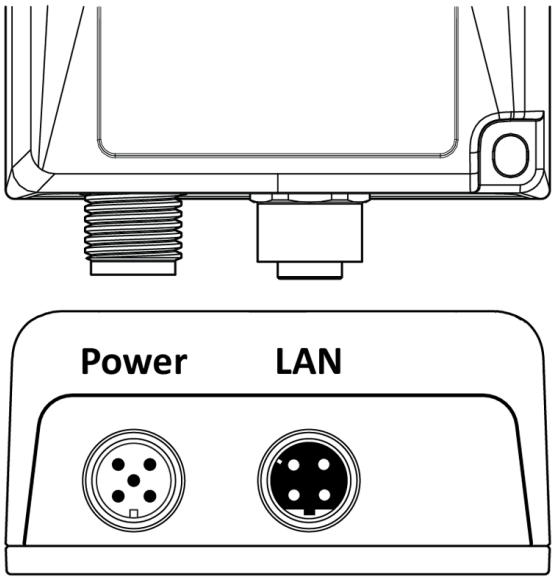
Digital Input Considerations
Digital input is used for additional functionality with advanced configurations and to remotely reset the unit.

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

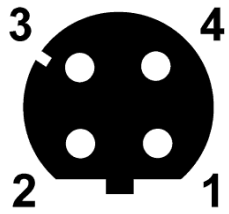
IMPORTANT
If wiring length exceeds 3 meters, signal wiring for the digital input must be carried in the same cable as power and functional earth.

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

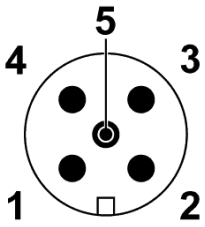
Procedure



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).

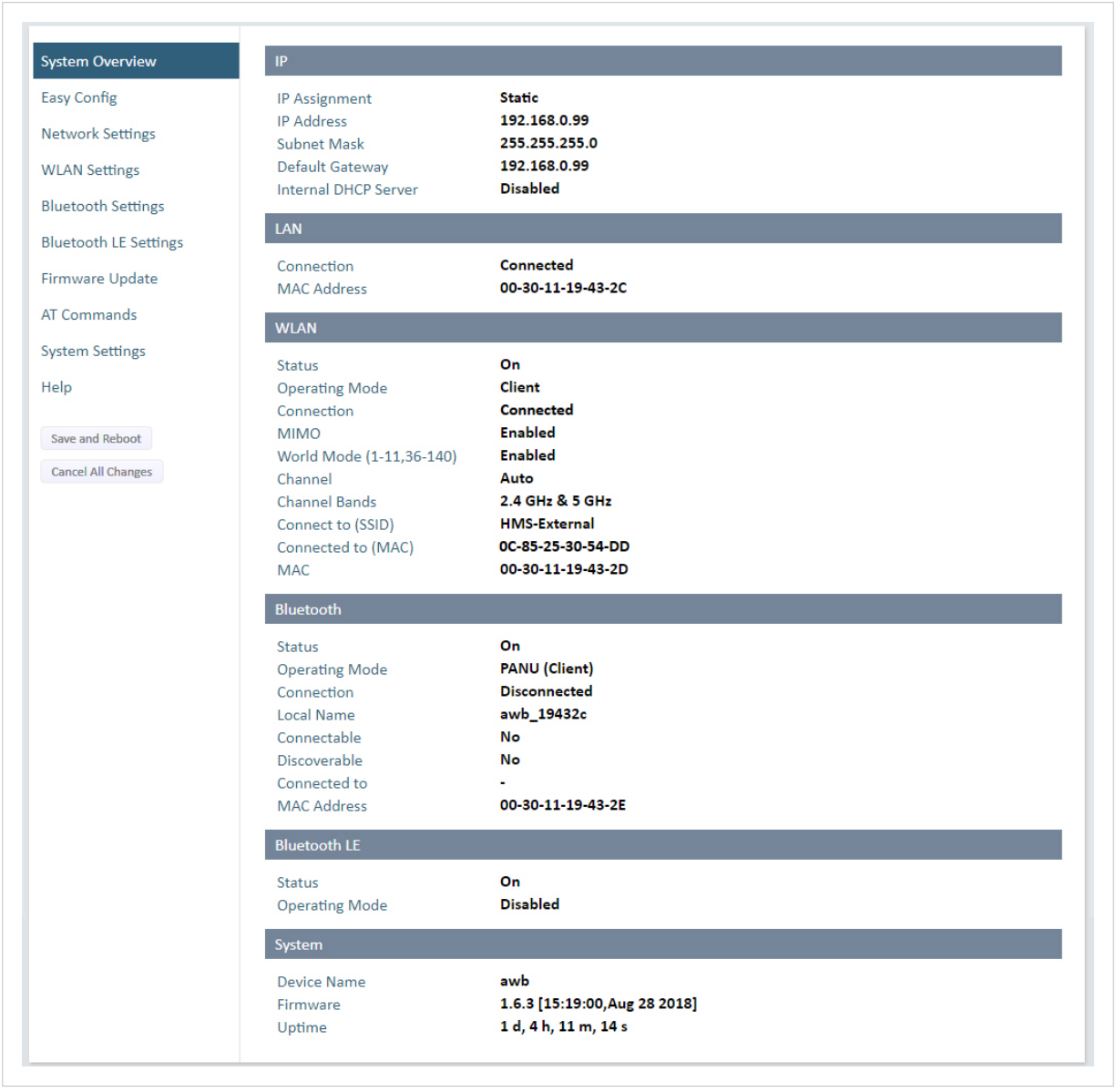


Figure 8. System Overview page example

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

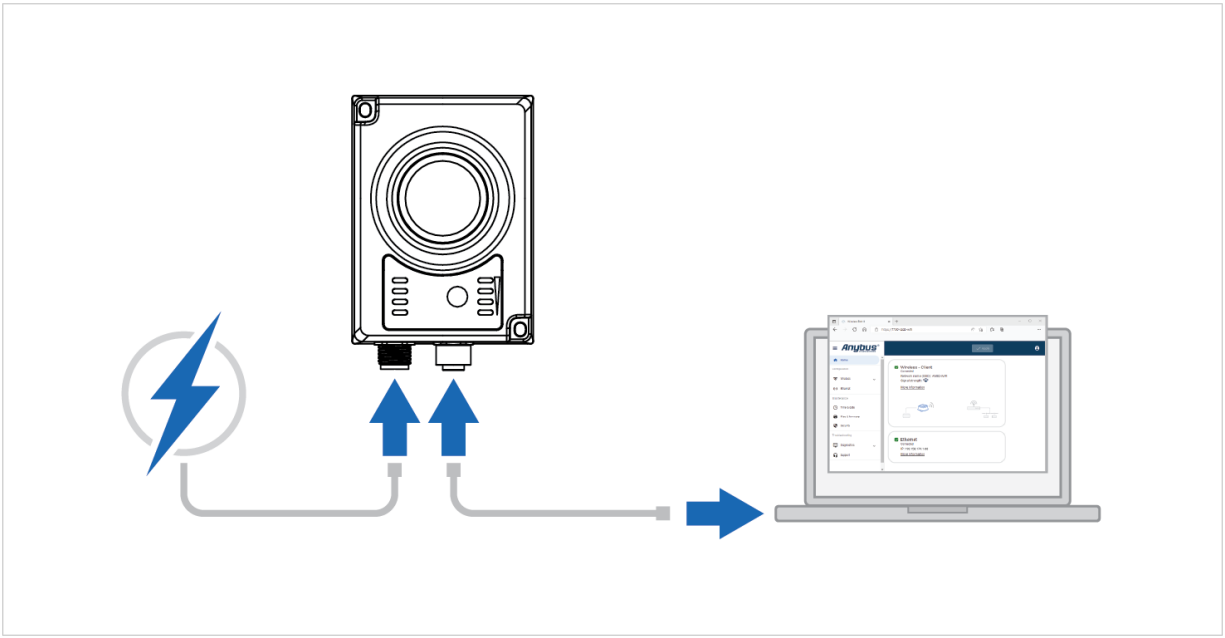


Figure 9. Connect to PC and Power

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.

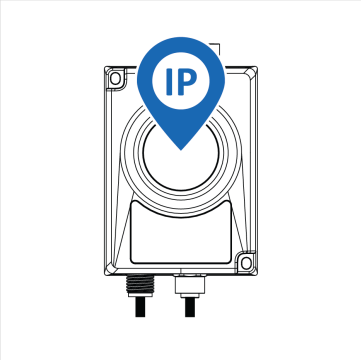
NOTE
The Bridge II Ethernet default IP address is 192.168.0.99 and the subnet mask is 255.255.255.0.

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.

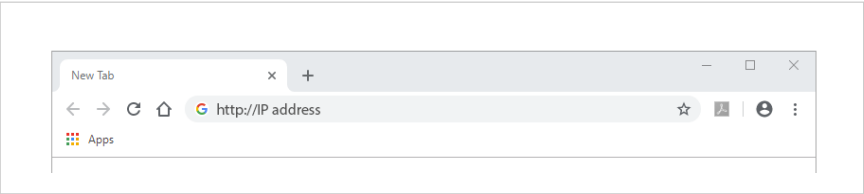


Figure 10. Enter IP address in web browser

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

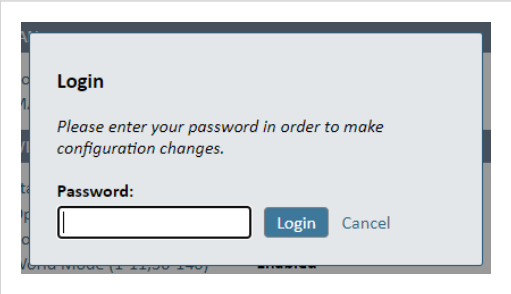


Figure 11. Built-in web interface login screen

Result

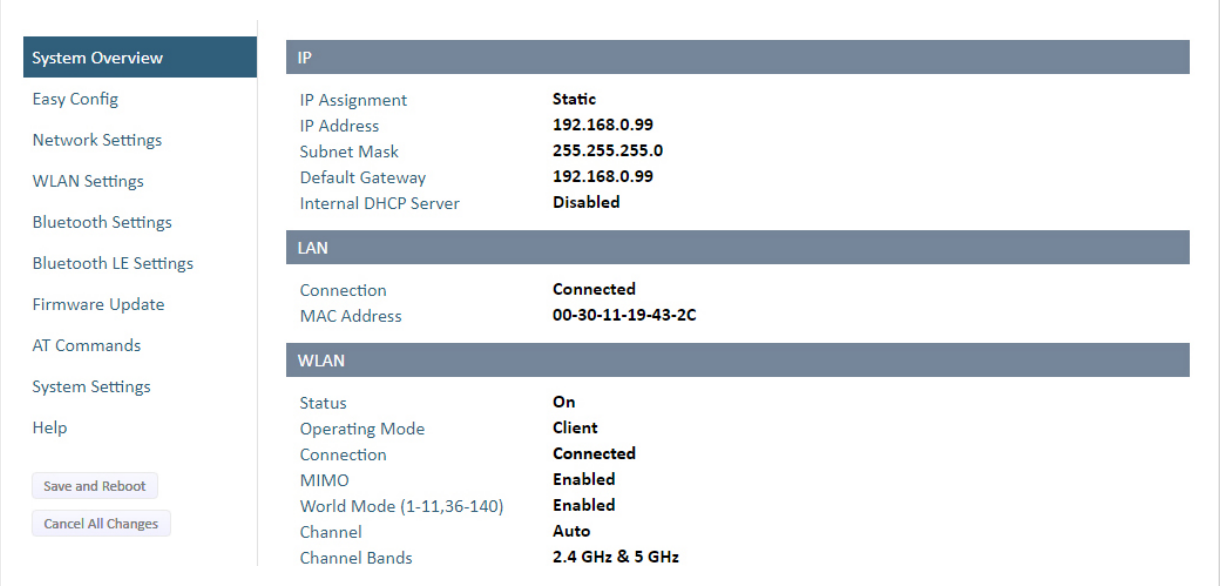
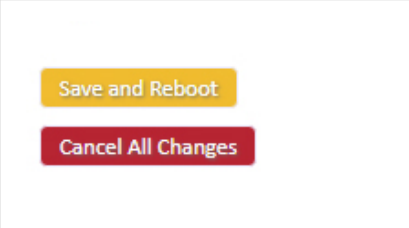


Figure 12. page

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)

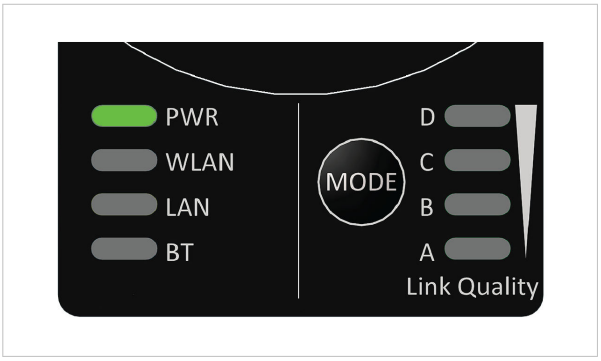


Figure 13. Easy Config A-B-C-D LED indicators

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.

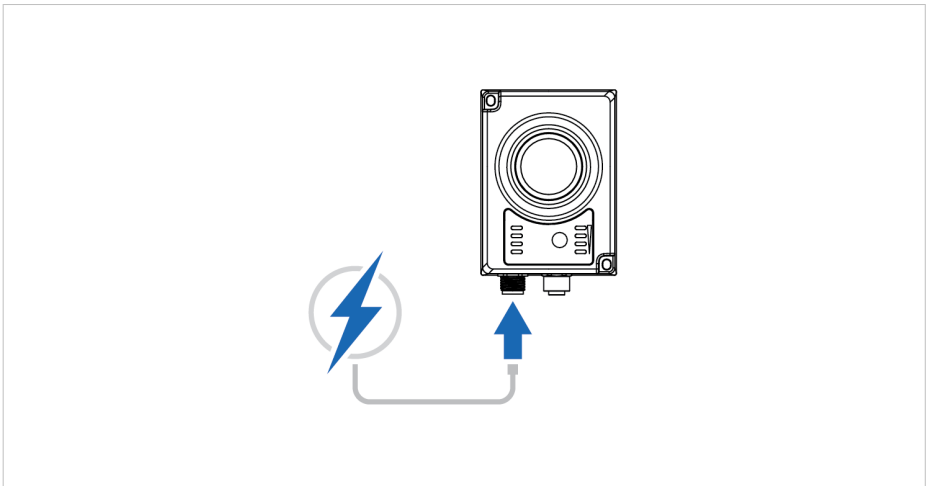


Figure 14. Connect to power

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

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

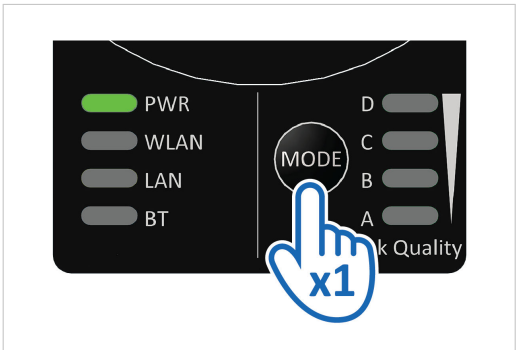


Figure 15. Press and release **MODE**

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

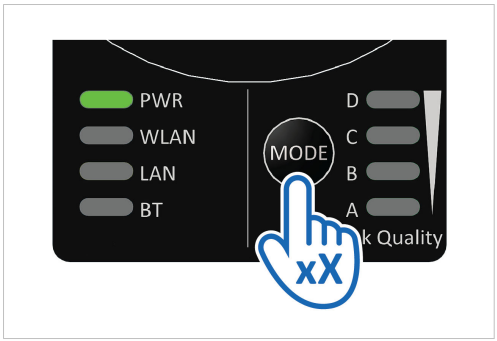


Figure 16. Select the desired mode

   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.

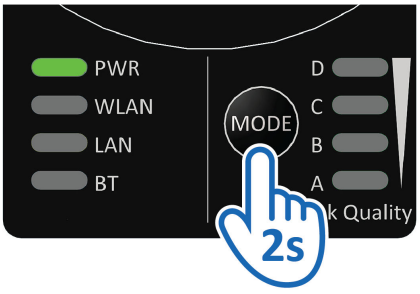


Figure 17. Confirm Easy Config mode

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.

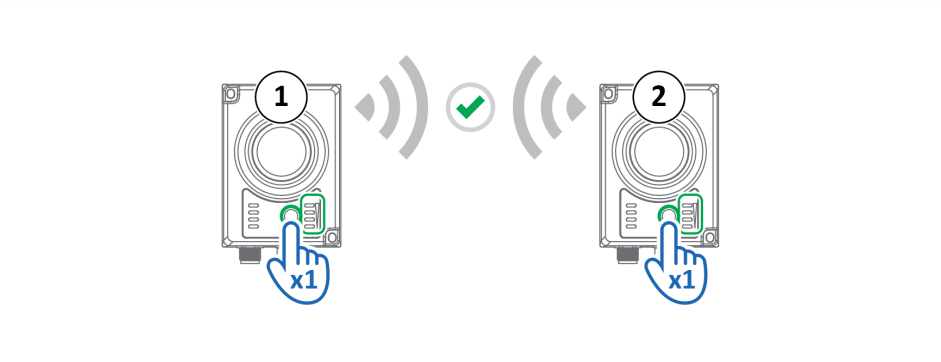


Figure 18. Codes match, Accept

- 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

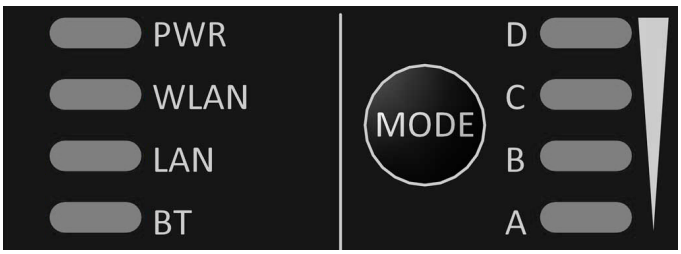


Figure 21. Status LED indicators

- 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

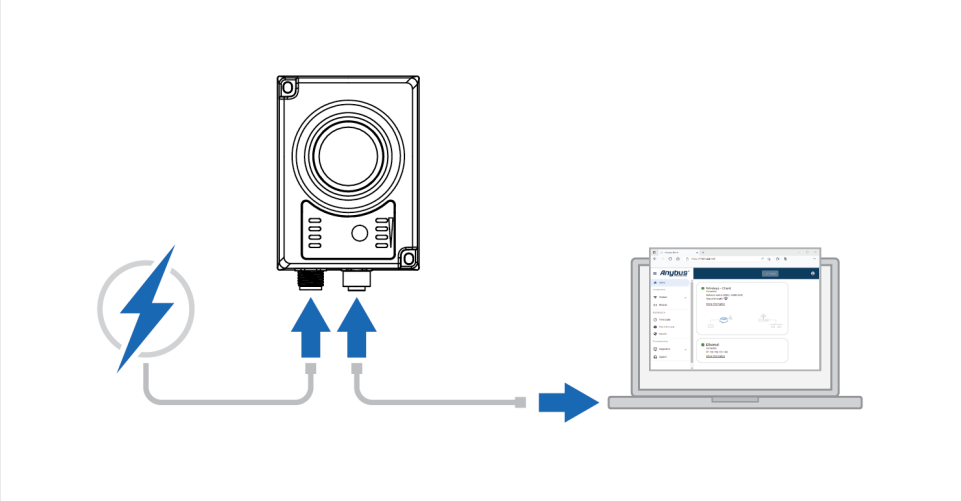


Figure 22. Connect to PC and power

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.

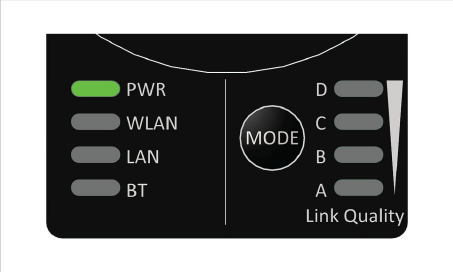


Figure 23. PWR LED

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.

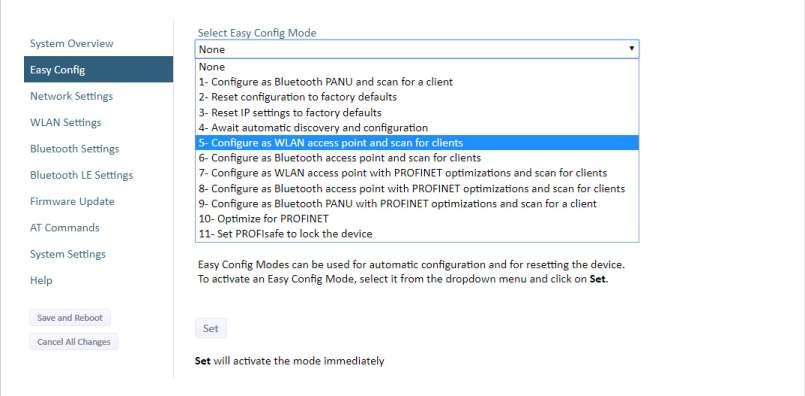


Figure 24. Easy Config Modes menu

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.

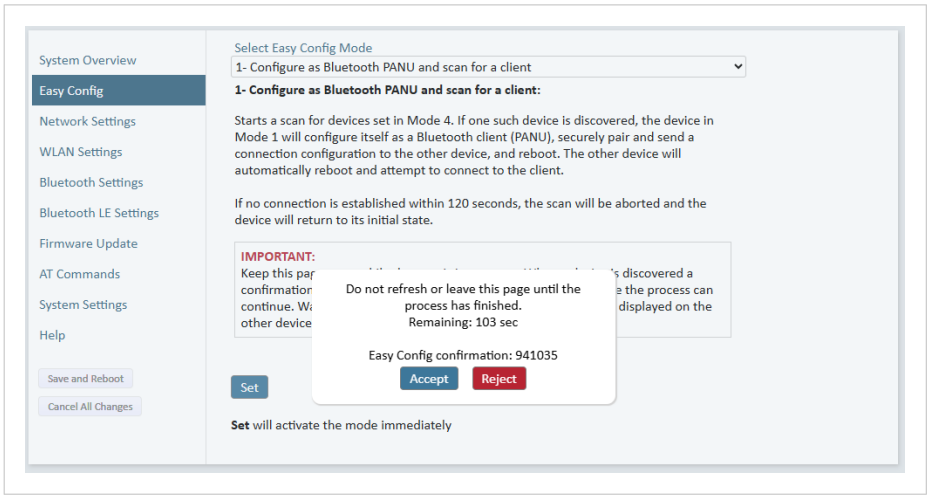


Figure 25. Easy Config page, confirmation dialog window

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.

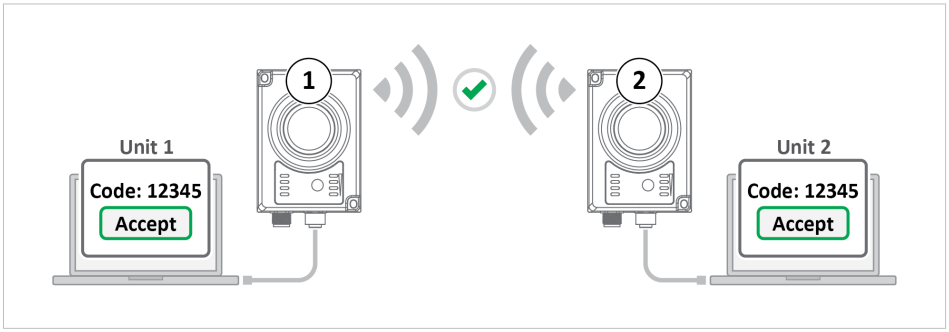


Figure 26. Codes match, Accept

- 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

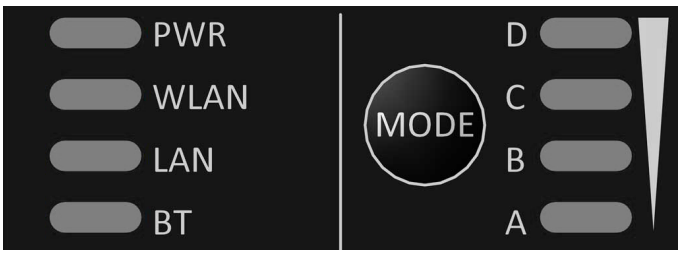


Figure 29. Status LED indicators

- 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

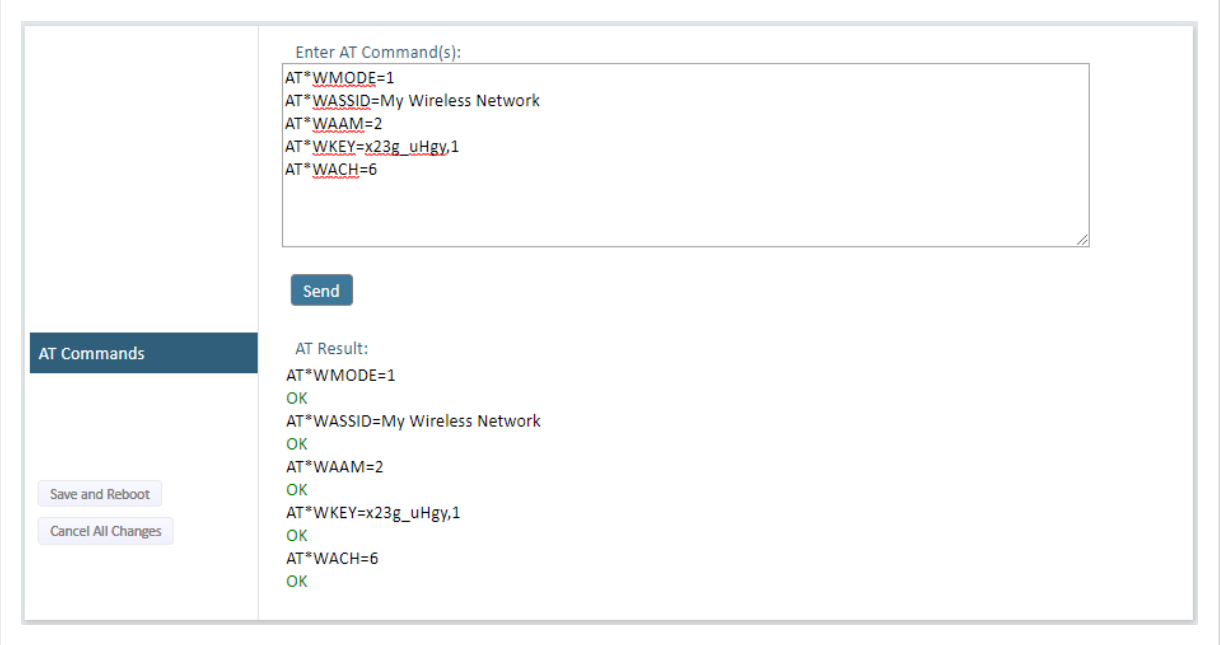


Figure 30. AT Commands and AT Results

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

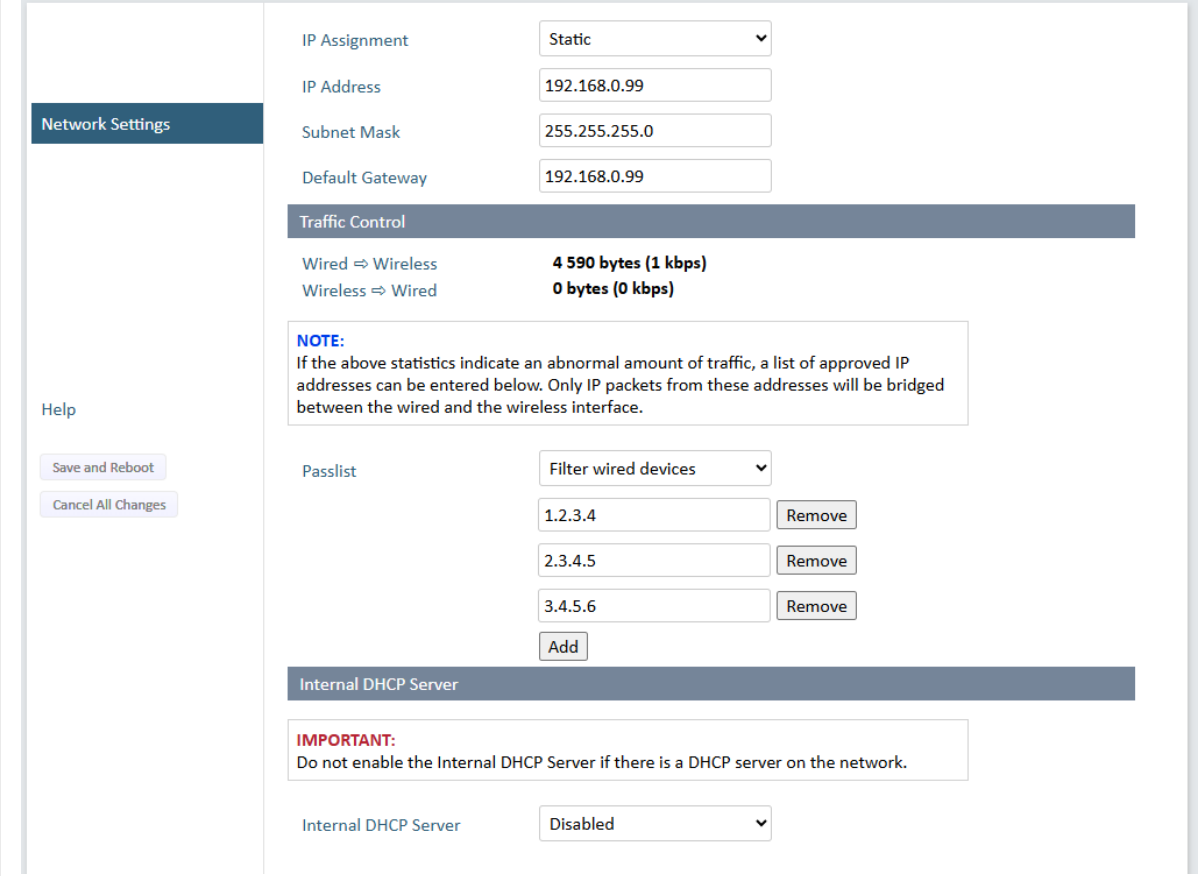


Figure 31. Network Settings page

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

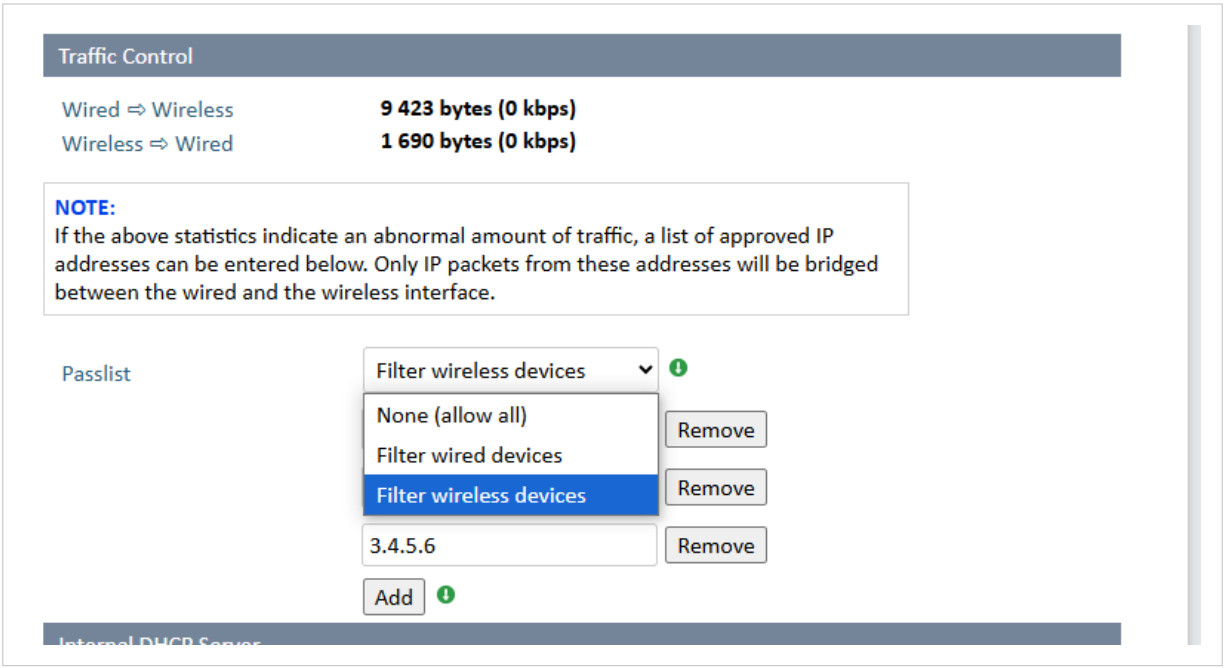


Figure 32. Network Settings, Traffic Control

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

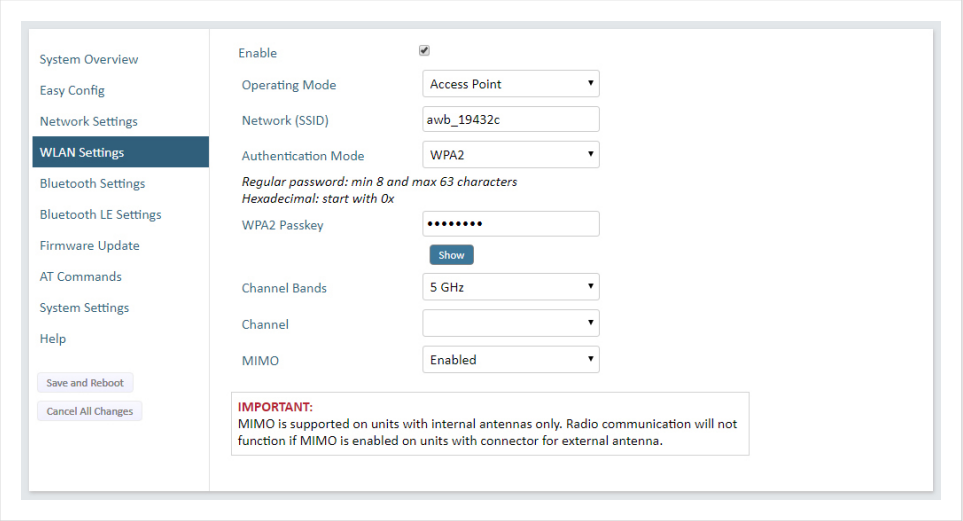


Figure 35. WLAN Settings page

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

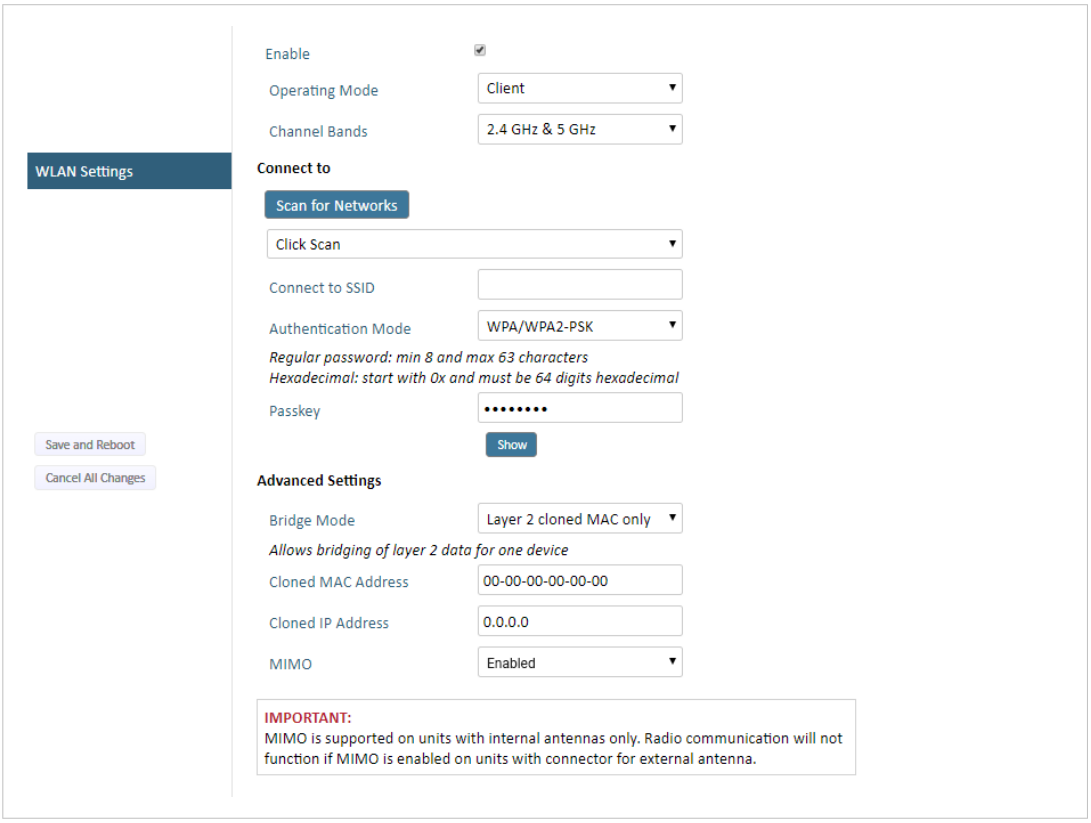


Figure 36. WLAN Settings page

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

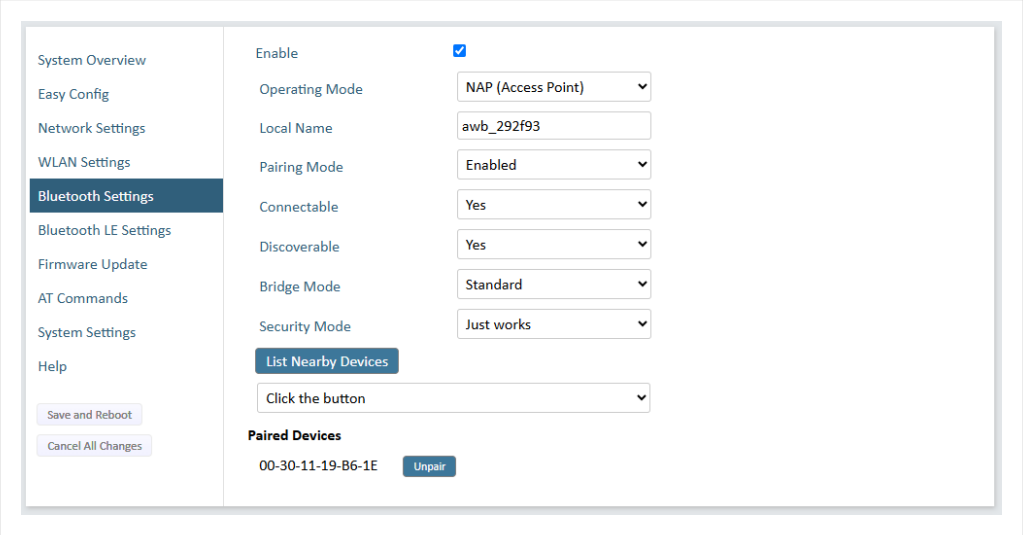


Figure 37. Bluetooth Settings page

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

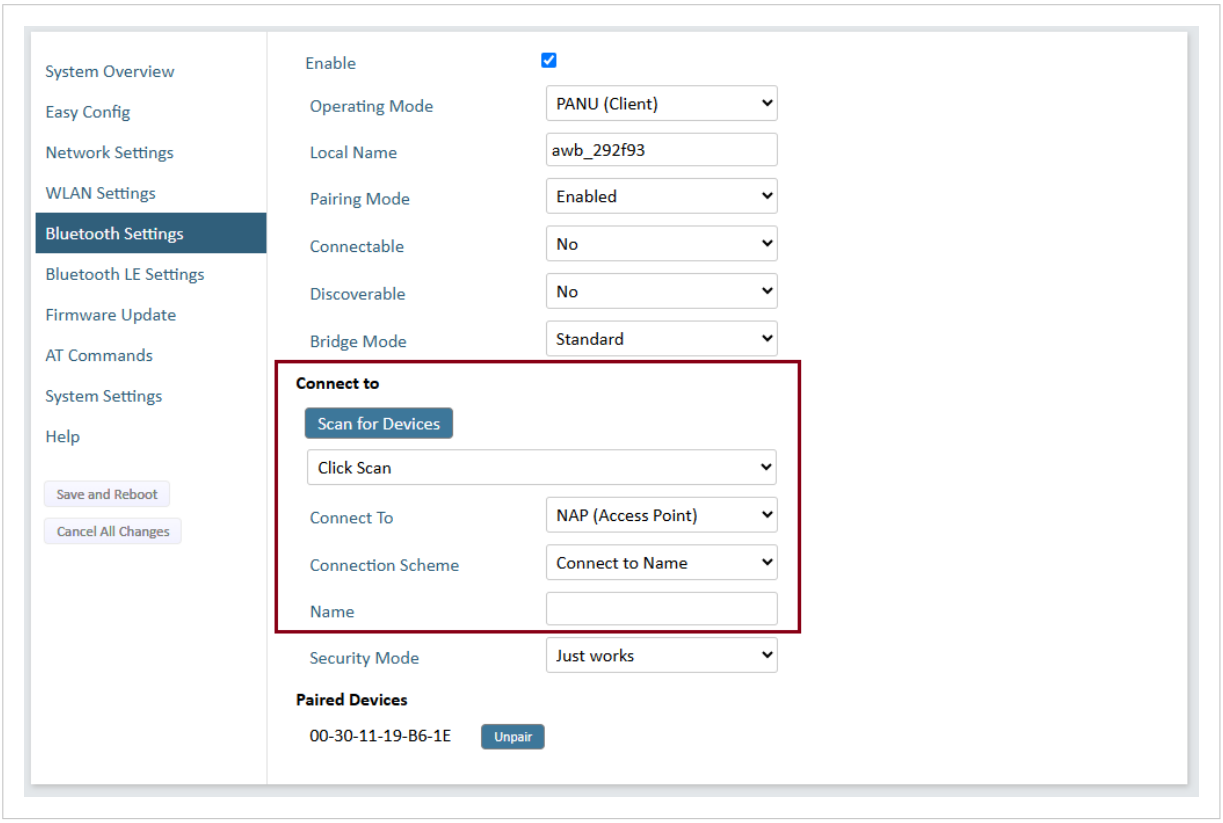


Figure 38. Bluetooth Settings page

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

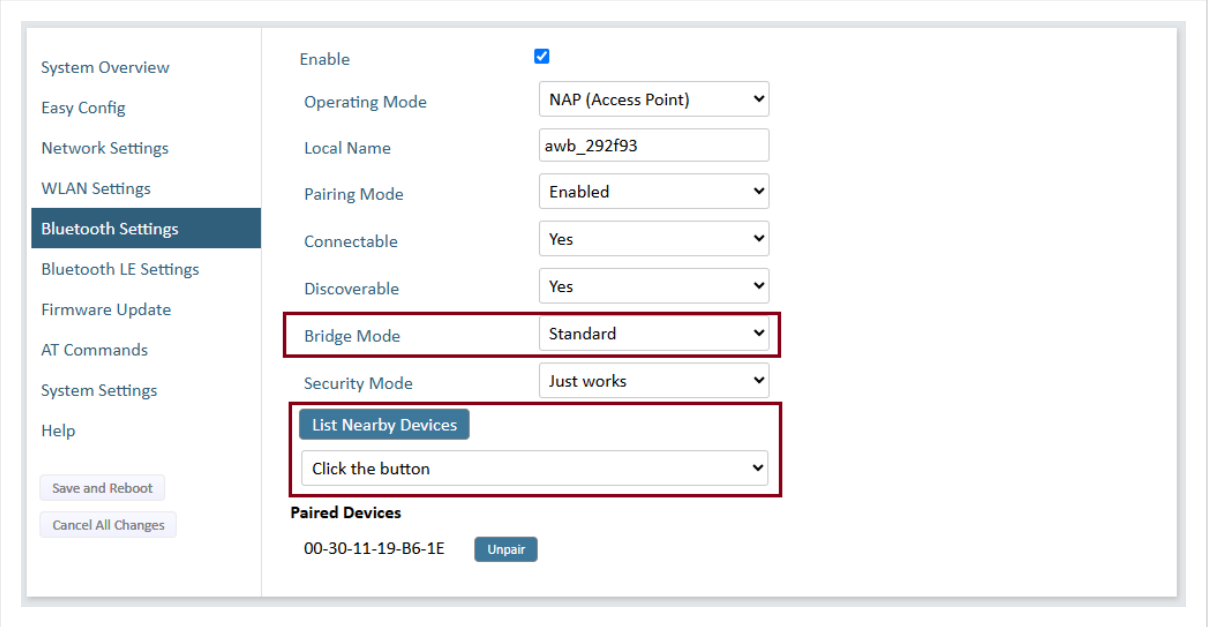


Figure 39. Bluetooth Settings page

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.

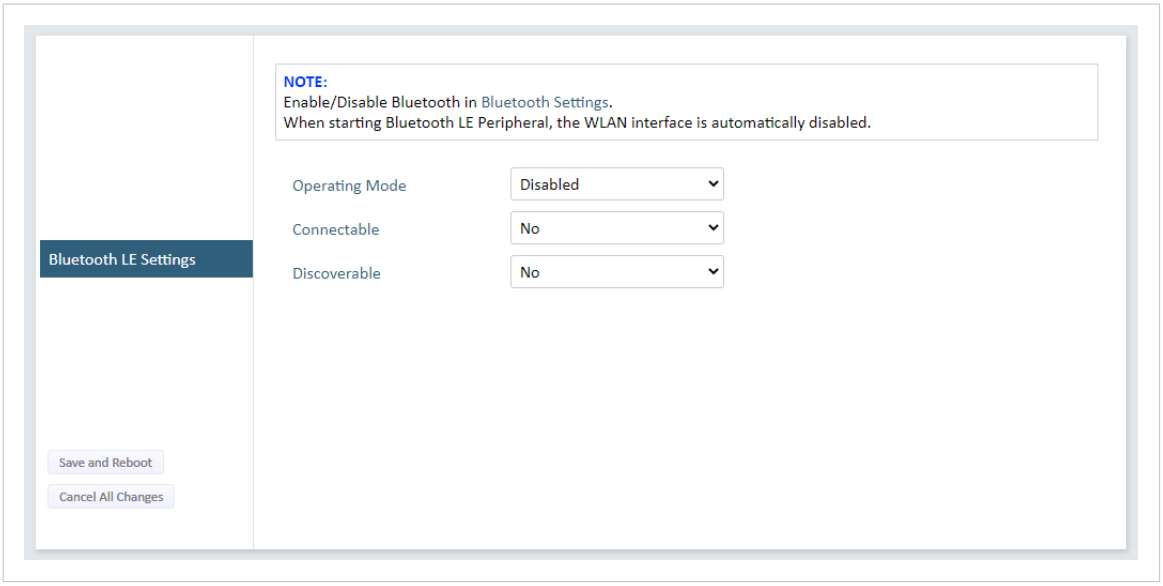


Figure 40. **Bluetooth LE Settings** page

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.

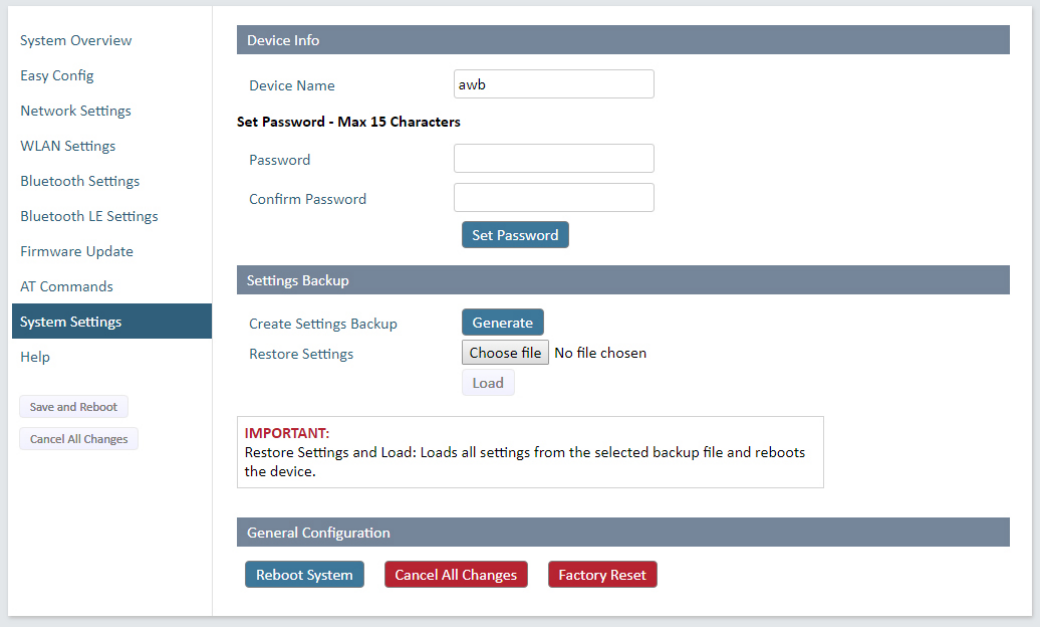


Figure 41. System Settings page

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.

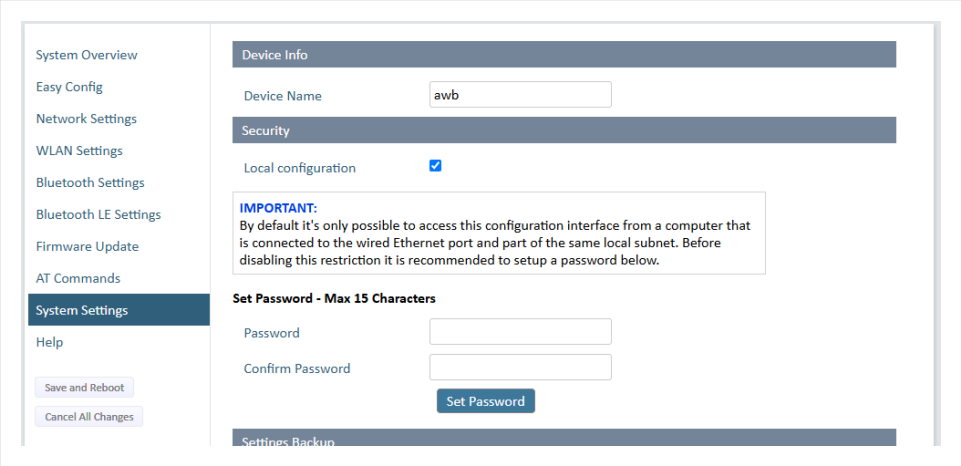


Figure 42. System Settings page, Security, Local configuration

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.

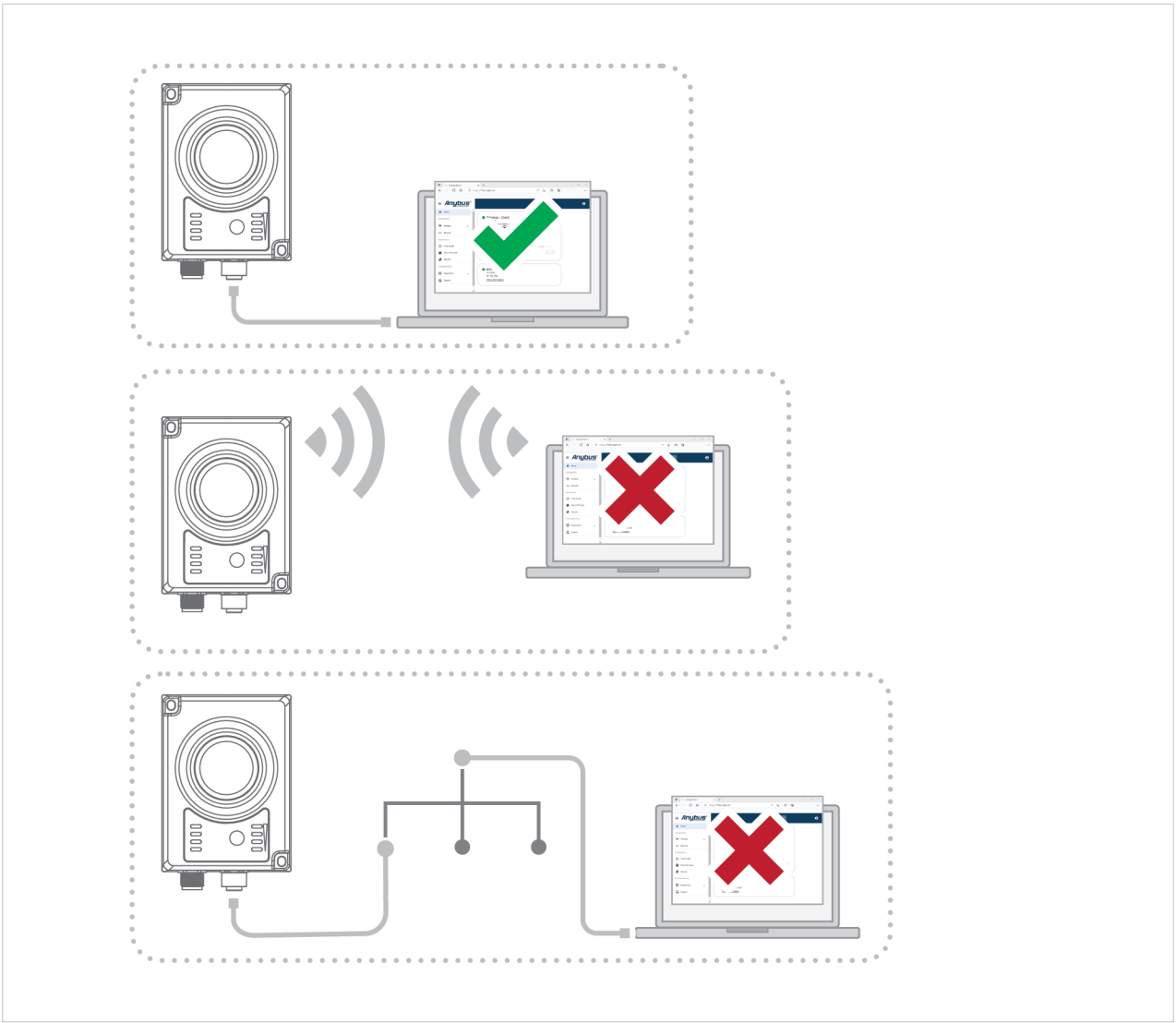


Figure 43. Direct LAN connection required for Bridge II Ethernet built-in web interface access

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

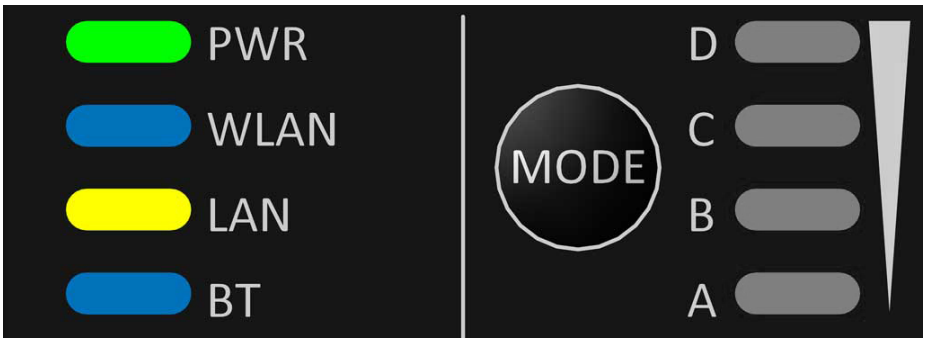


Figure 44. Status LED indicators

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.

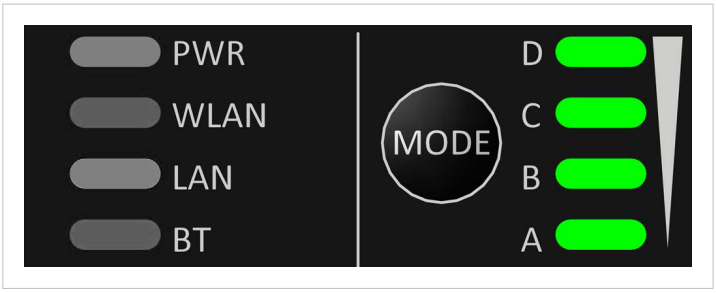


Figure 45. Link Quality/Mode indicators

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.

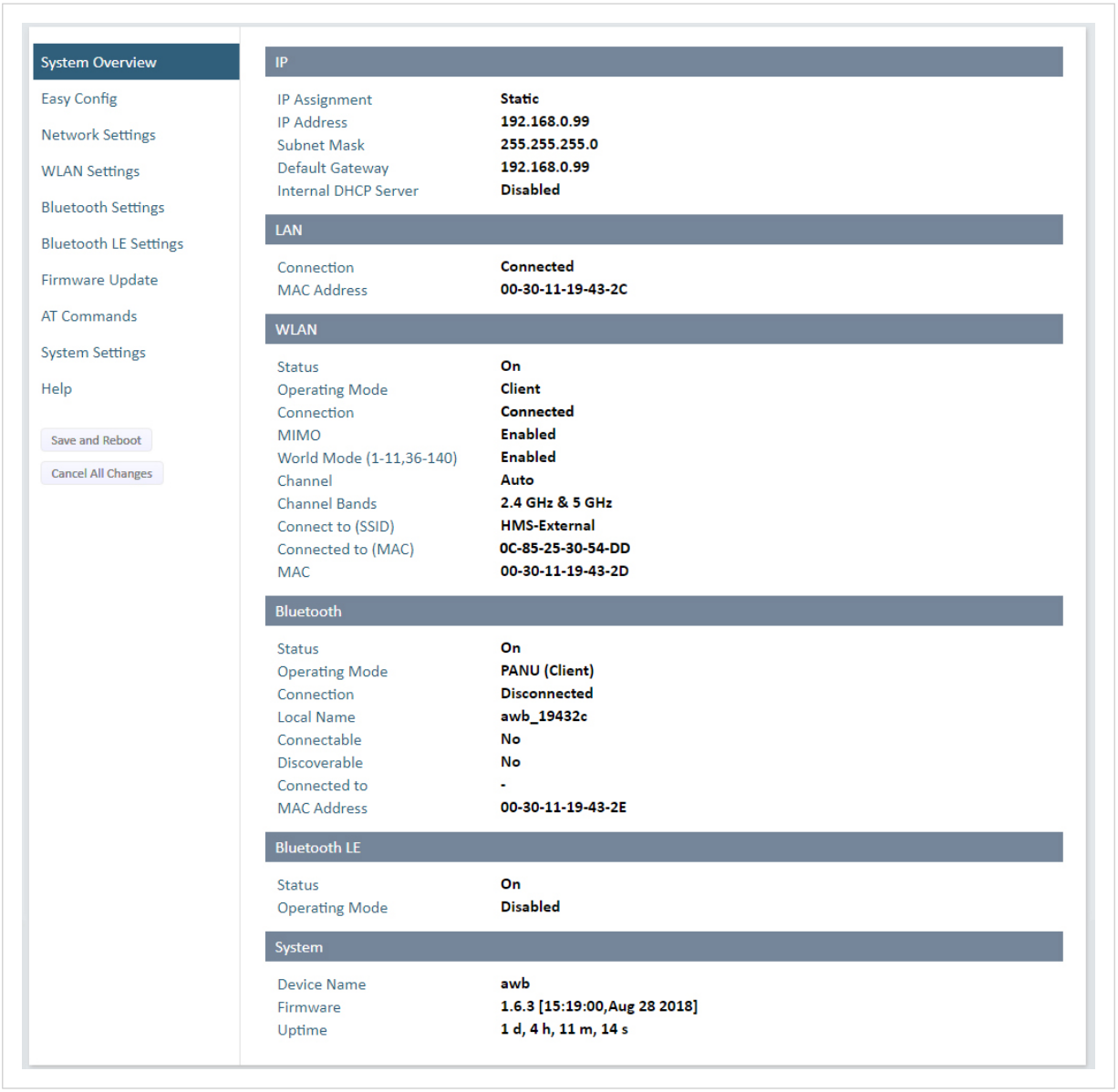


Figure 46. System Overview page example

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

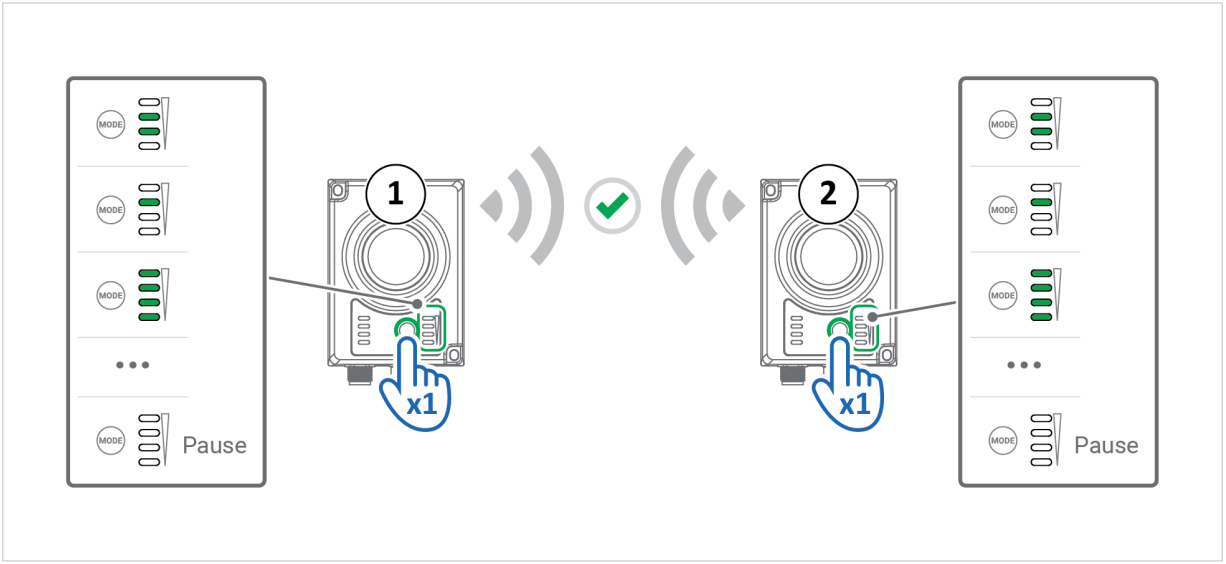


Figure 47. Codes match, Accept

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

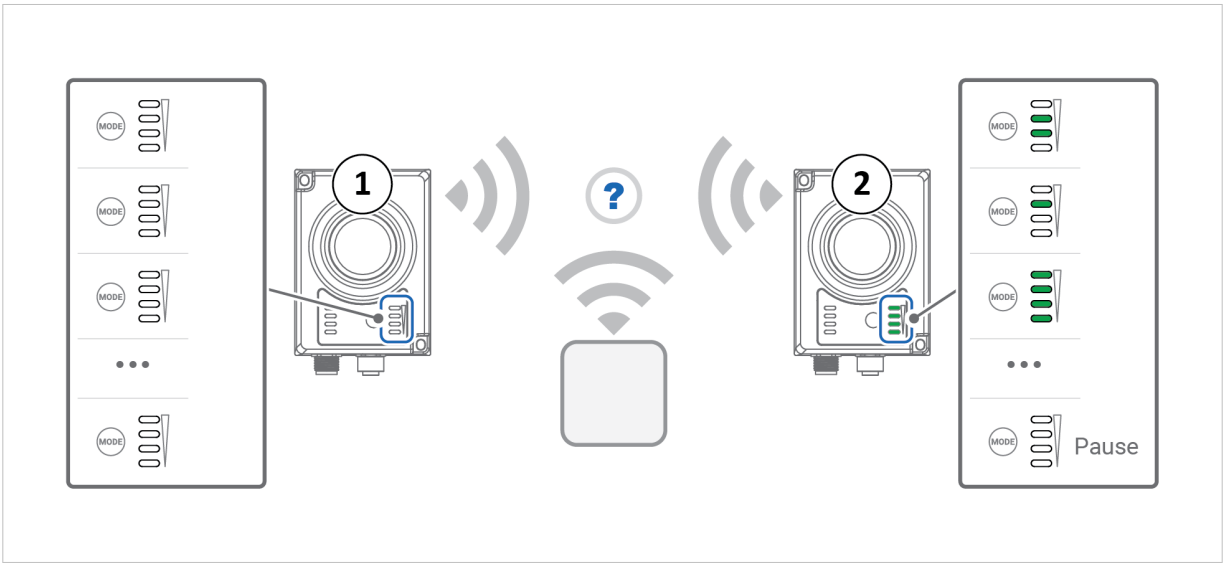


Figure 48. LED indicators blink on one unit only, wait for the Easy Config mode to timeout

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

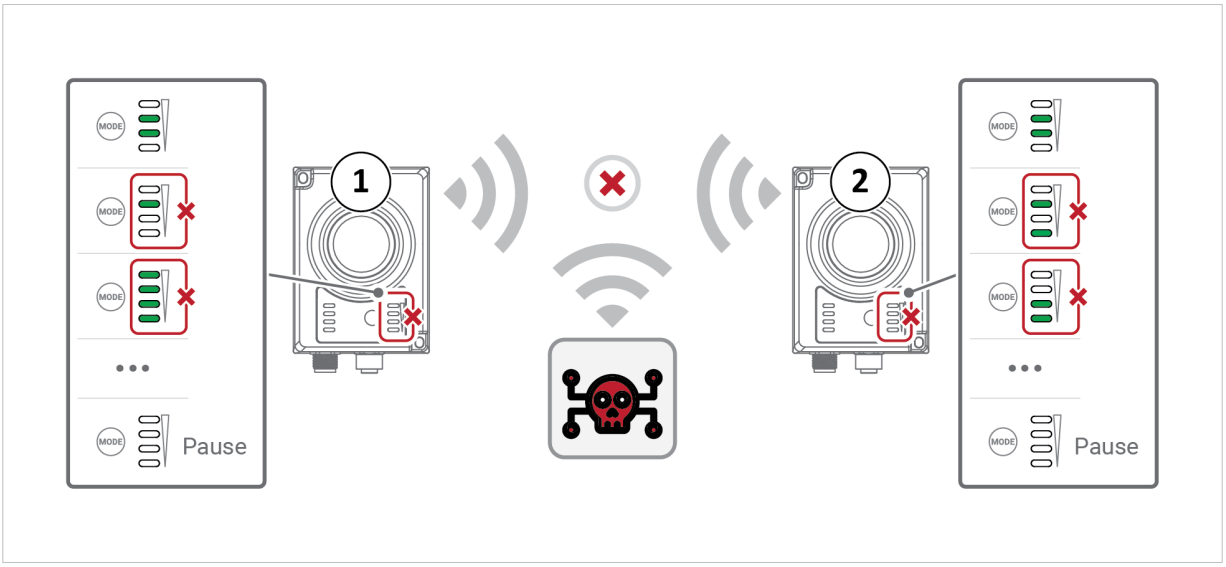


Figure 49. LED indicators blinking patterns do not match, wait for the Easy Config mode to timeout

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

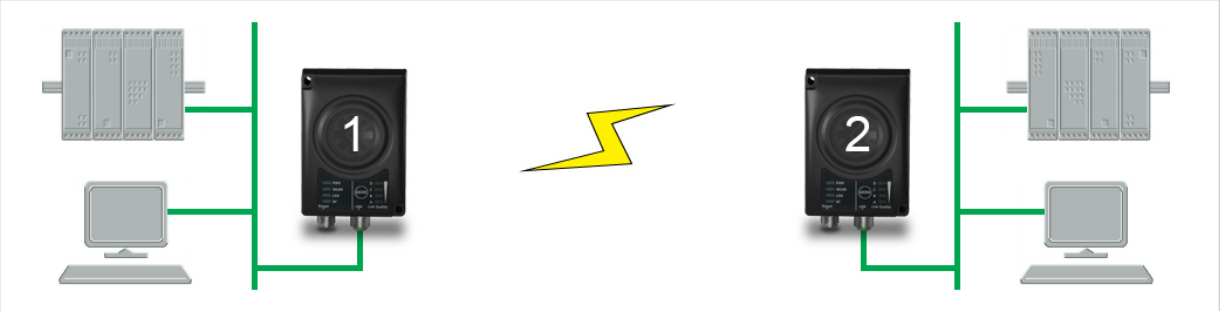


Figure 50. Ethernet bridge

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

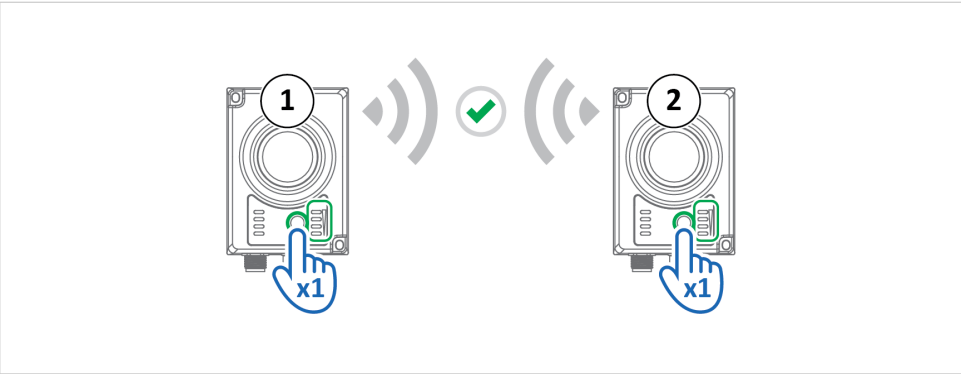


Figure 51. Codes match, Accept

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

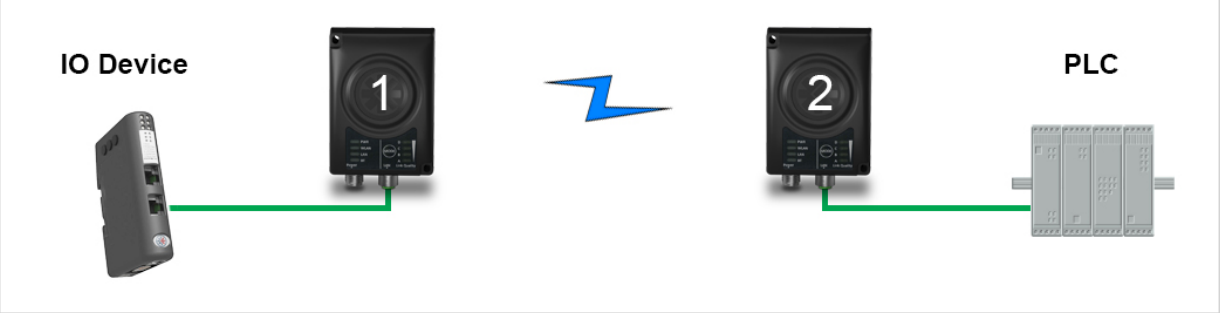


Figure 52. PROFINET wireless network

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

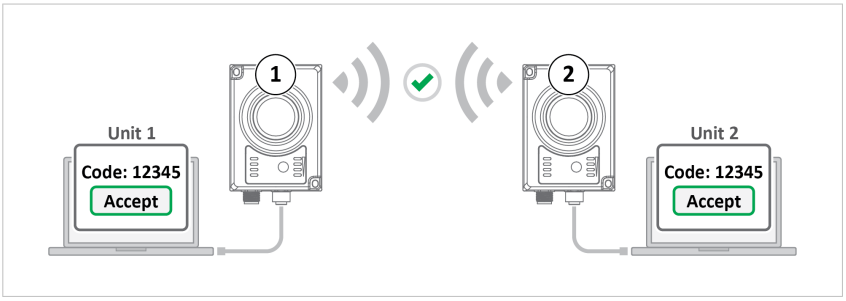
The Bridge II Ethernets are configured with PROFINET optimization. This means that PROFINET messages have priority over TCP/IP frames.

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

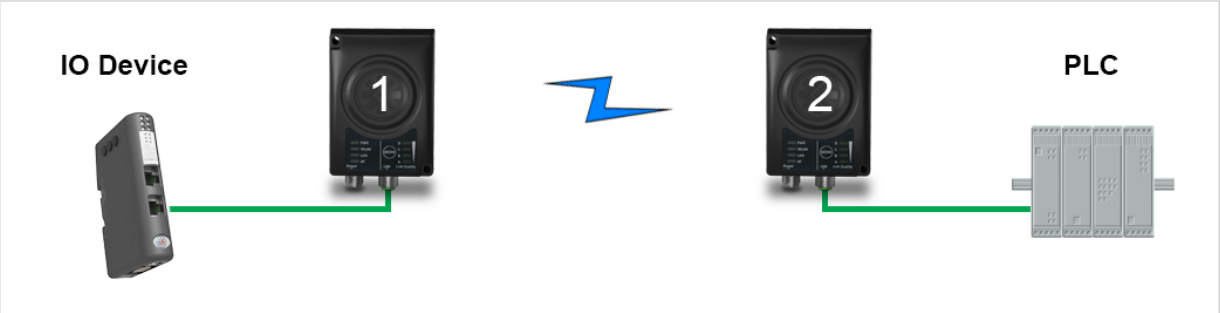


Figure 53. EtherNet/IP wireless network

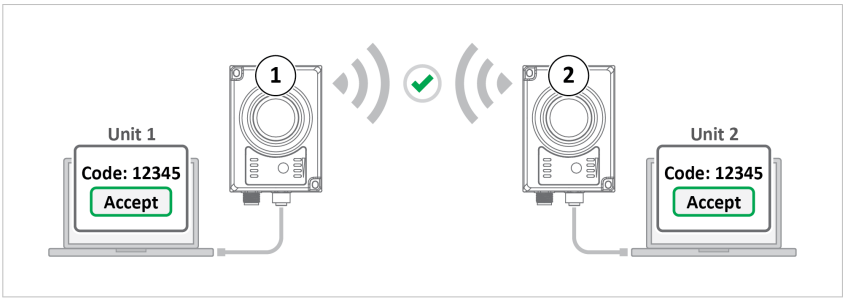
This example describes how to connect an EtherNet/IP IO device and an EtherNet/IP PLC over Bluetooth using two Wireless Bridges and Easy Config.

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**.

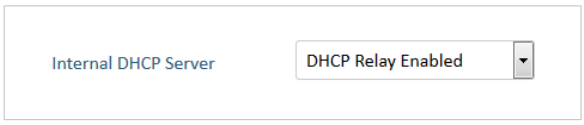


Figure 55. DHCP Relay Enabled

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**.

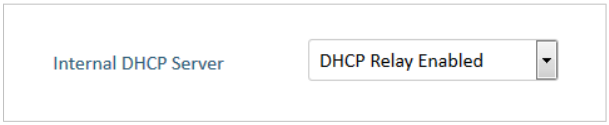


Figure 58. DHCP Relay Enabled

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.

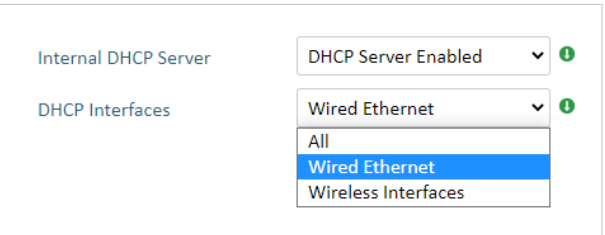


Figure 59. DHCP Interfaces, Wired Ethernet

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

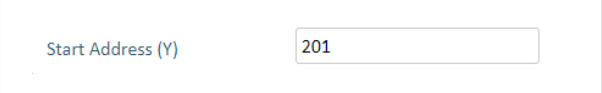


Figure 60. Start Address for DHCP addressing

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**.

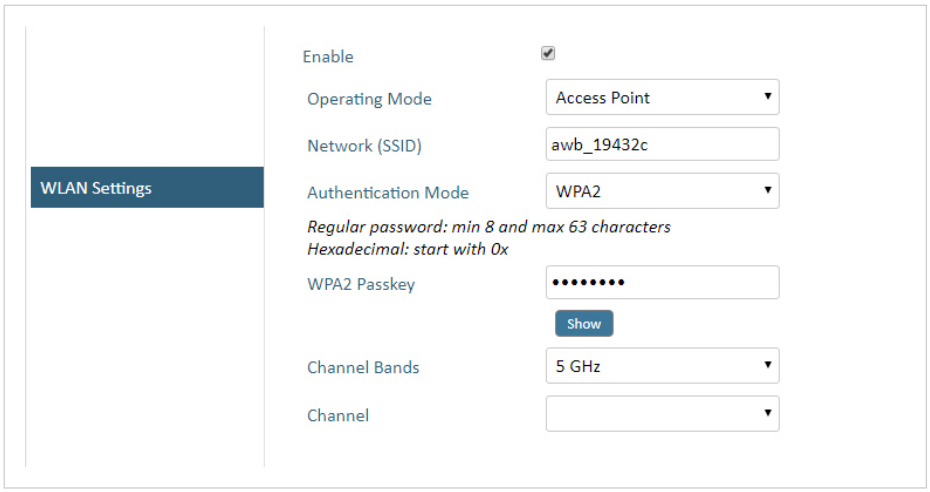


Figure 61. WLAN Settings

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.

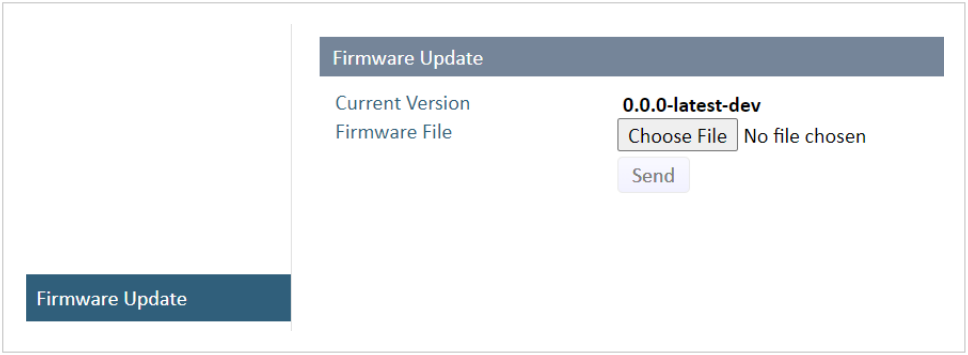


Figure 62. Firmware Update, Choose file

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

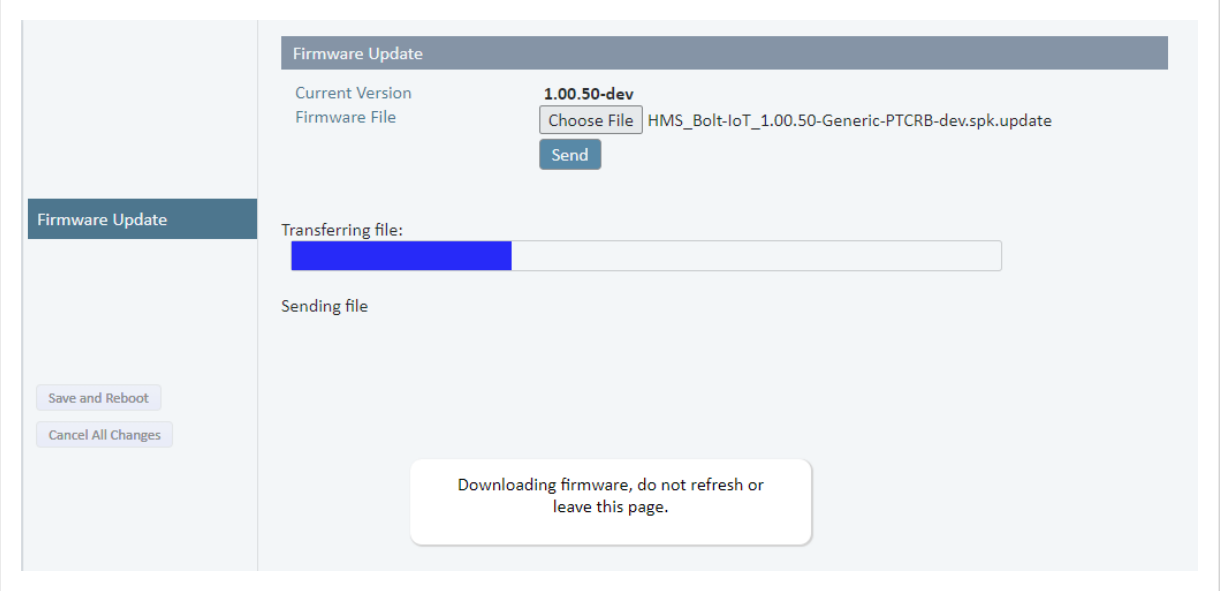


Figure 63. Firmware Update, Transferring file

- 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

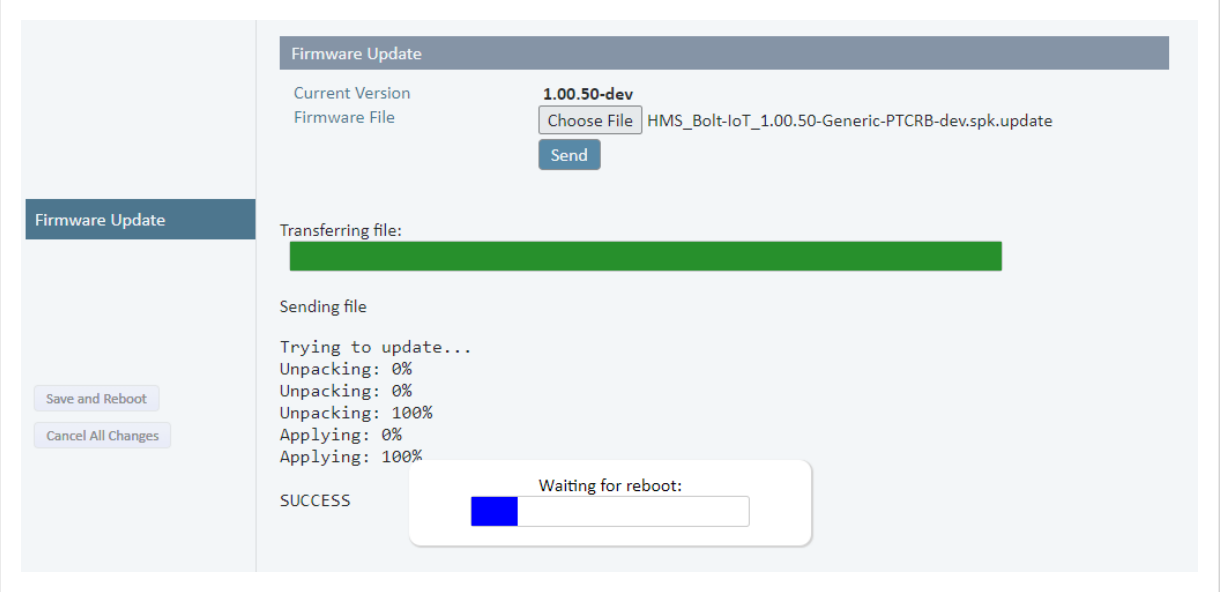


Figure 64. Firmware Update, Waiting for reboot

- 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**.

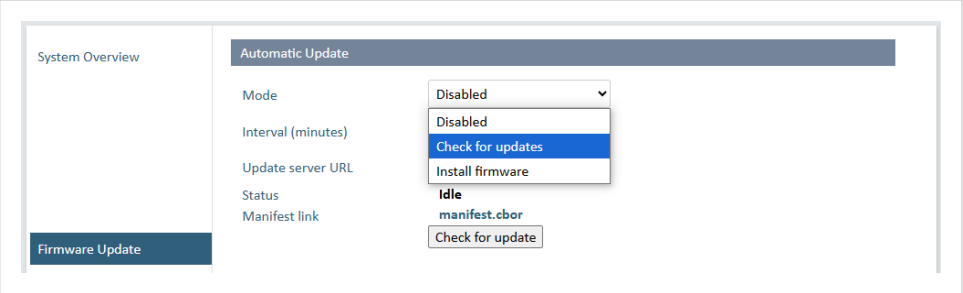


Figure 65. Automatic Update Mode menu, Check for updates

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).

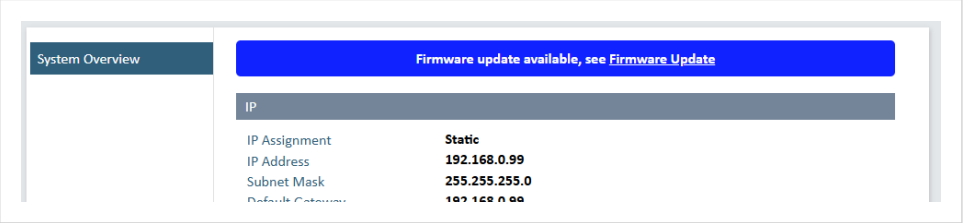


Figure 66. Firmware update available banner

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**.

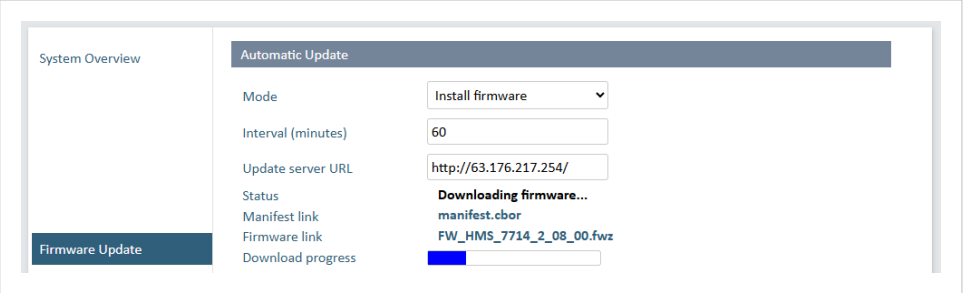


Figure 67. Automatic Update Mode menu, Install firmware

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.

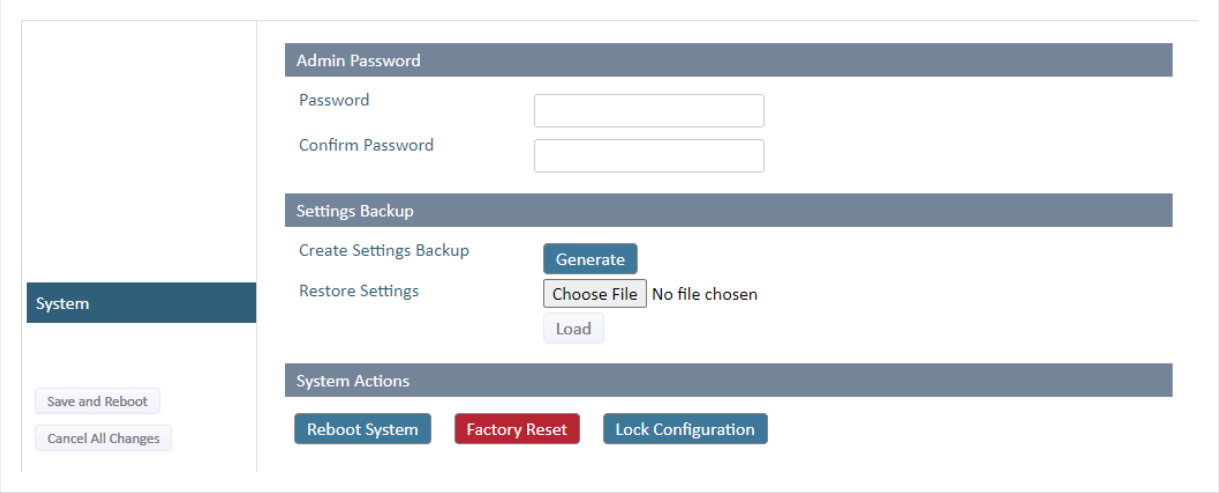


Figure 68. System page

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.

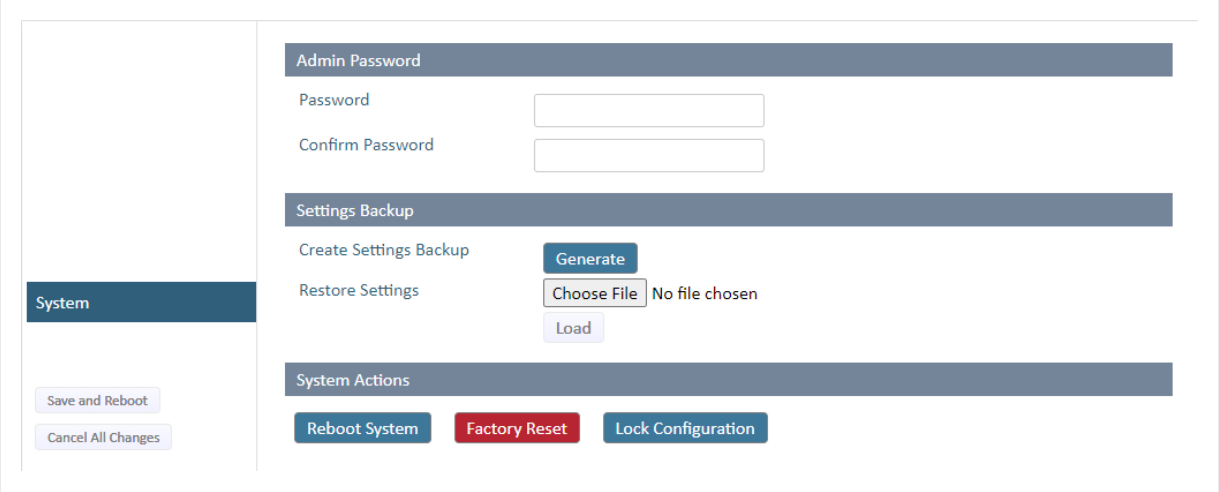


Figure 69. Restore Settings from a backup file

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.

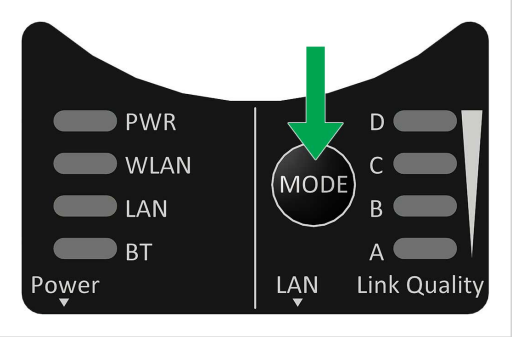


Figure 70. **MODE** button

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

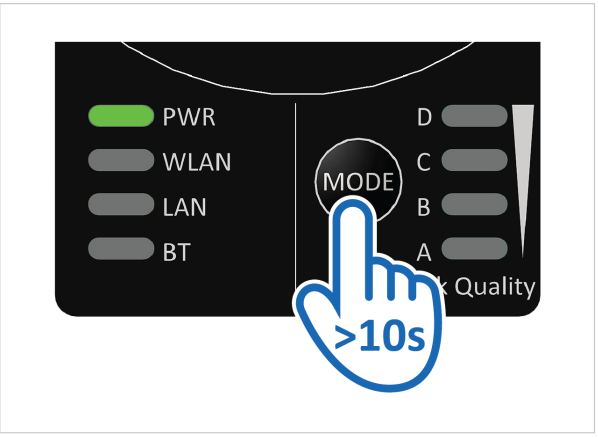
To Reinstall the Firmware

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

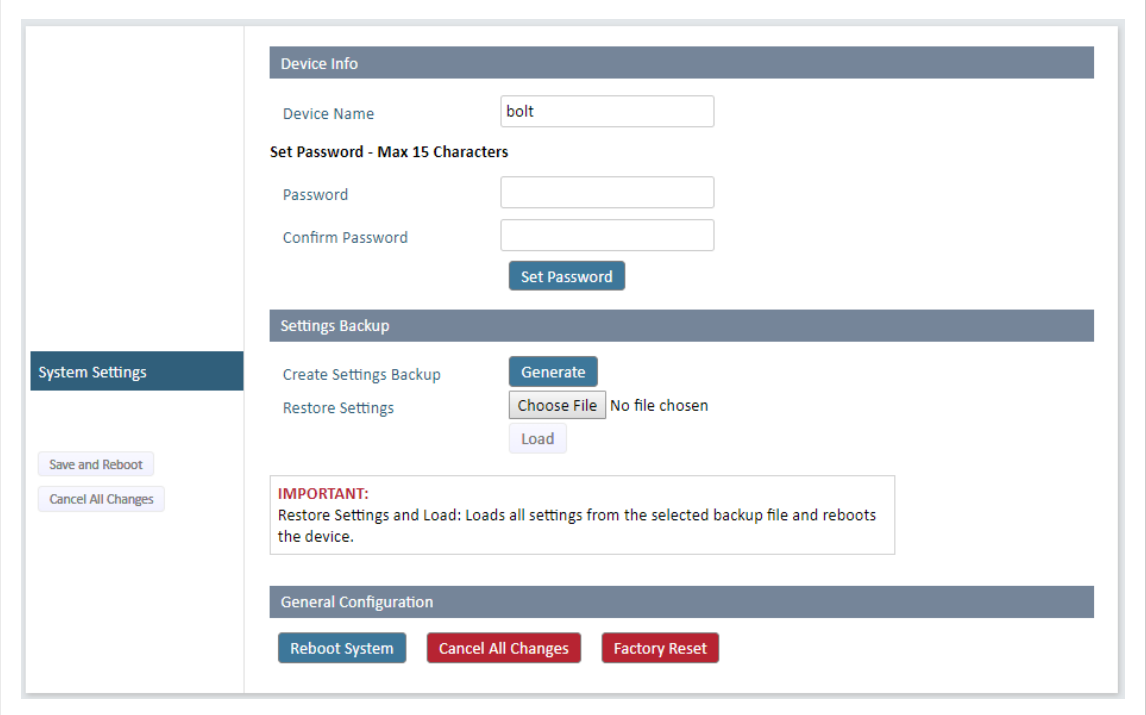
Any one of these actions will restore the unit to factory default settings.

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.

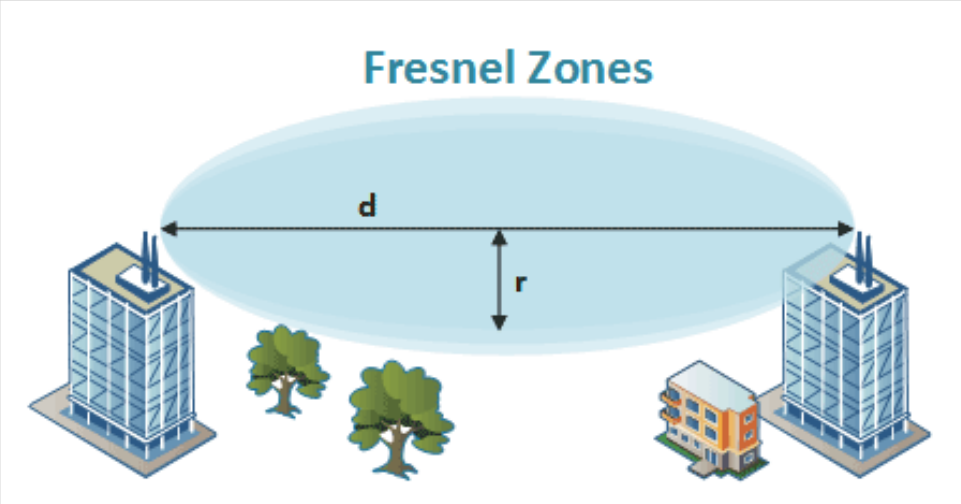


Figure 71. Fresnel zones

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.

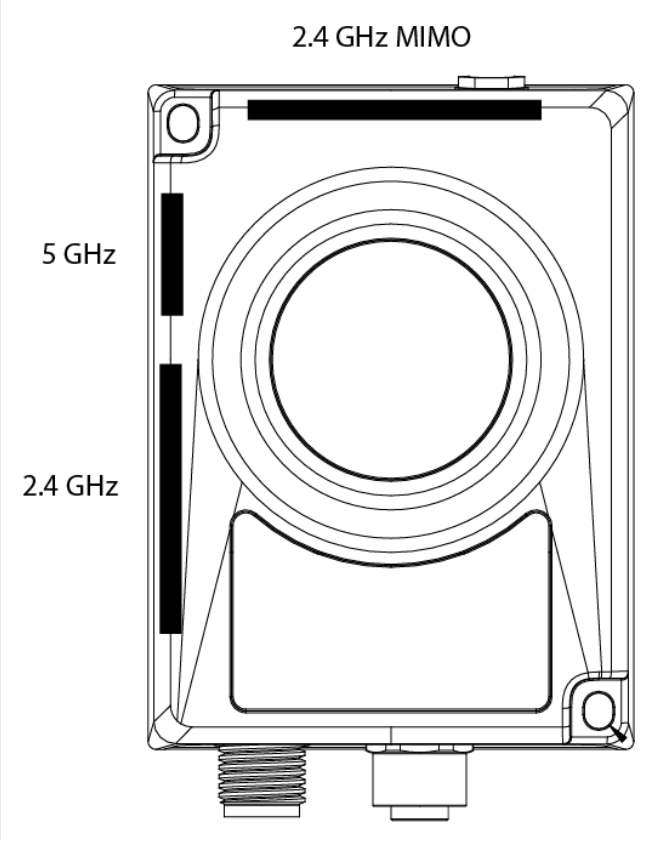
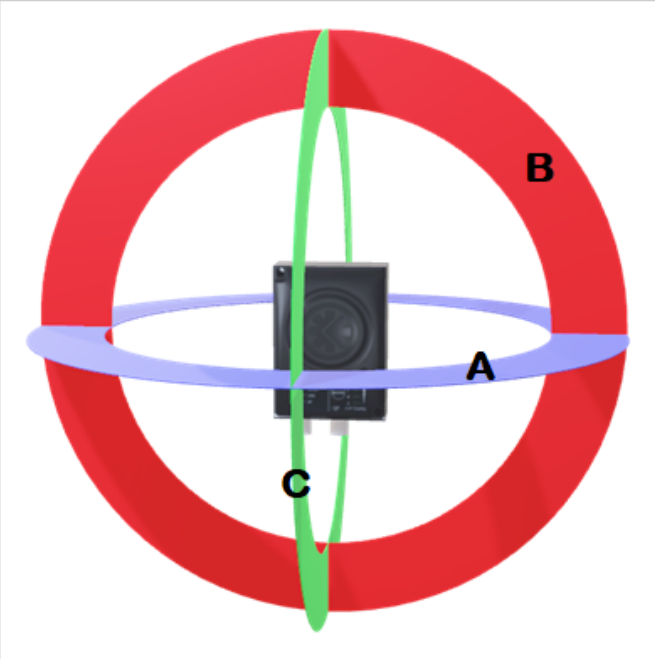


Figure 72. Placement of the three antennas in the unit

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

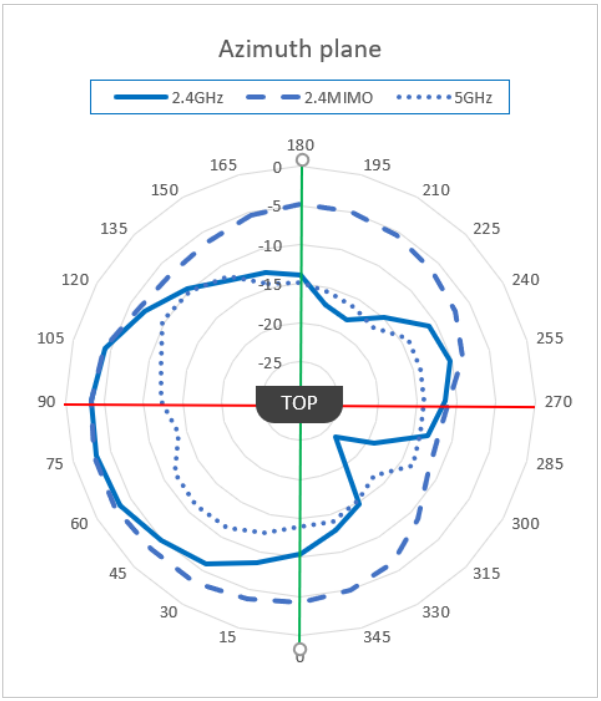


Figure 73. Azimuth plane

Front View – Elevation (Vertical)

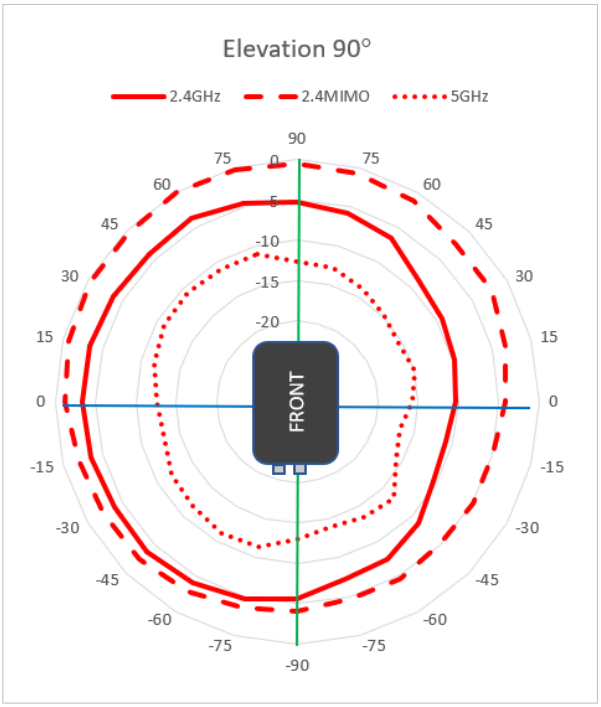


Figure 74. Elevation 90°

Side View – Elevation (Vertical)

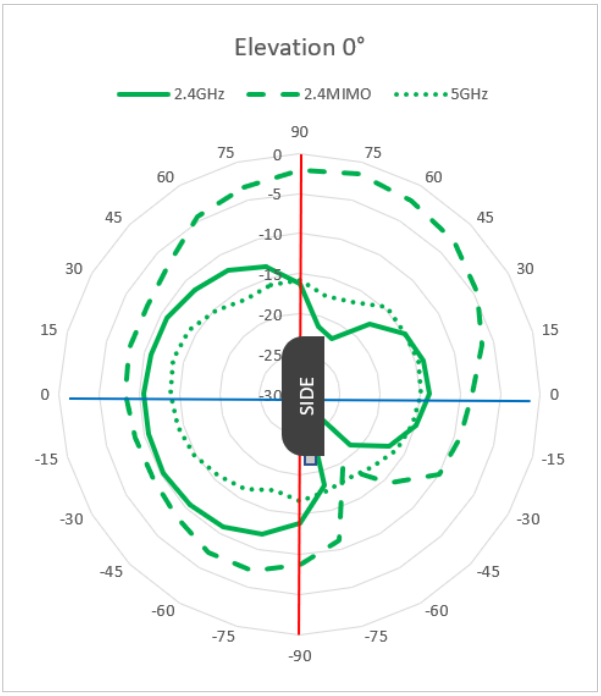


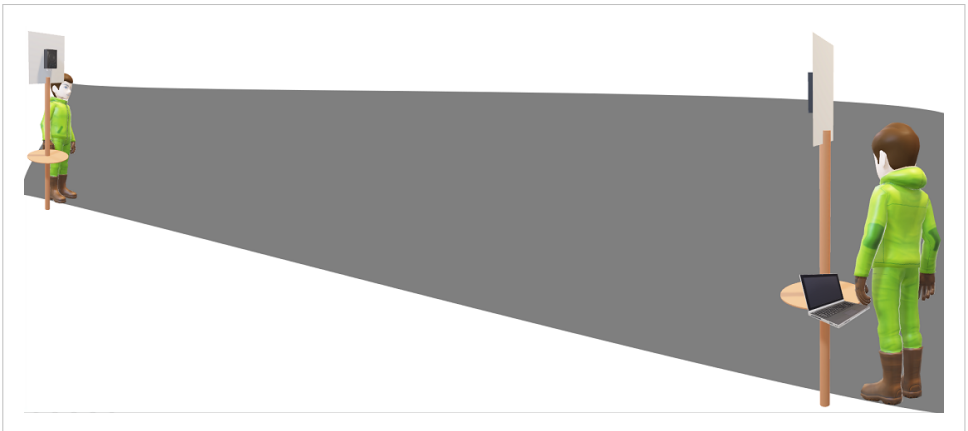
Figure 75. Elevation 0°

13.2.3. Real World Measurements

Azimuth (Horisontal) View with and without Back Shield

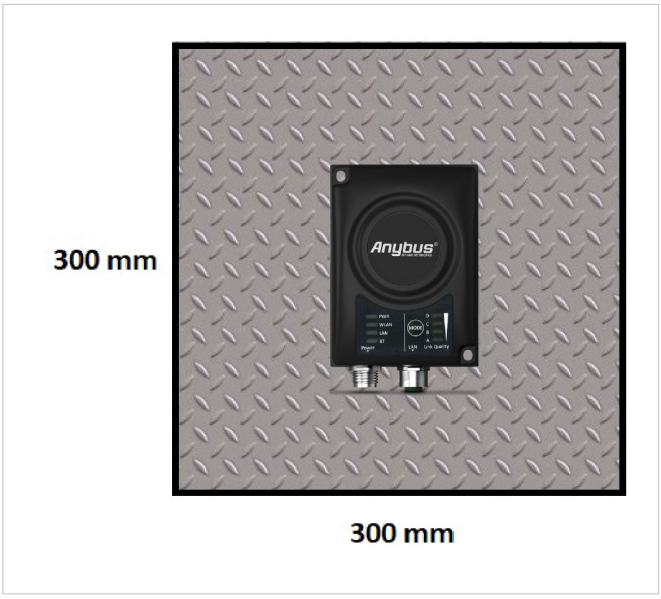
This pattern was measured in an outdoor environment, on an open field with no disturbing equipment or radiation.

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



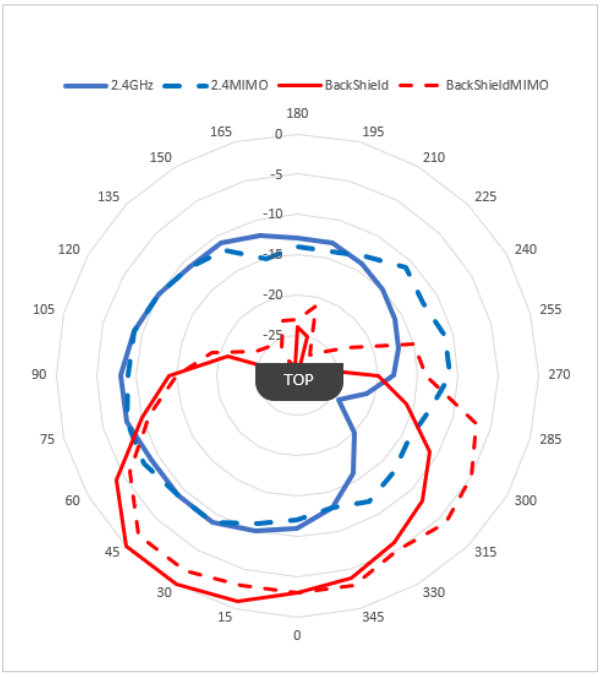
In this example, the measurements are made both with and without back shield.

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).

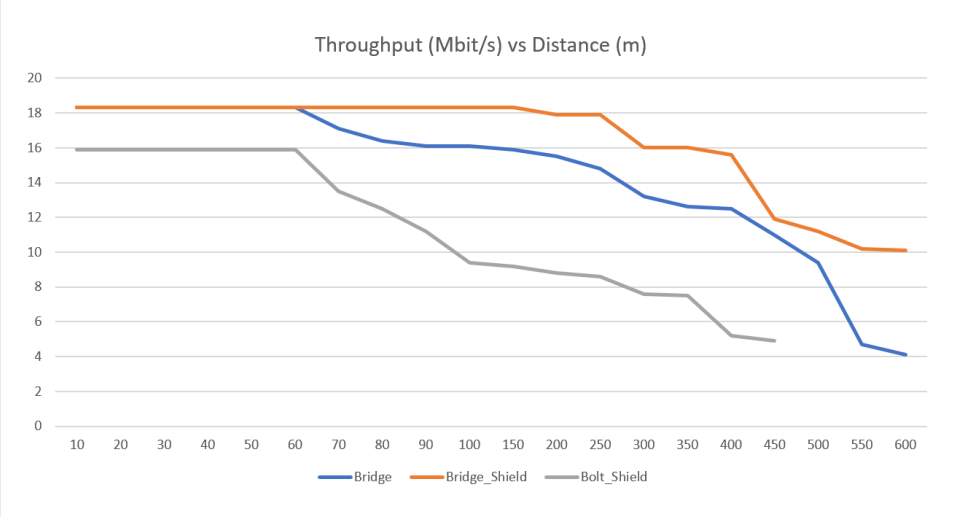
Figure 78. Measurements with and without back shield

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

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