Anybus® Wireless Bolt™

USER MANUAL

SCM-1202-007 1.0 ENGLISH



HMS Connecting Devices™

Important User Information

Liability

Every care has been taken in the preparation of this document. Please inform HMS Industrial Networks AB of any inaccuracies or omissions. The data and illustrations found in this document are not binding. We, HMS Industrial Networks AB, reserve the right to modify our products in line with our policy of continuous product development. The information in this document is subject to change without notice and should not be considered as a commitment by HMS Industrial Networks AB. HMS Industrial Networks AB assumes no responsibility for any errors that may appear in this document.

There are many applications of this product. Those responsible for the use of this device must ensure that all the necessary steps have been taken to verify that the applications meet all performance and safety requirements including any applicable laws, regulations, codes, and standards.

HMS Industrial Networks AB will under no circumstances assume liability or responsibility for any problems that may arise as a result from the use of undocumented features, timing, or functional side effects found outside the documented scope of this 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.

The examples and illustrations in this document are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular implementation, HMS Industrial Networks AB cannot assume responsibility for actual use based on these examples and illustrations.

Intellectual Property Rights

HMS Industrial Networks AB has intellectual property rights relating to technology embodied in the product described in this document. These intellectual property rights may include patents and pending patent applications in the USA and other countries.

Trademark Acknowledgements

Anybus® is a registered trademark of HMS Industrial Networks AB. All other trademarks are the property of their respective holders.

Copyright © 2016 HMS Industrial Networks AB. All rights reserved.

Table of Contents

Page

1 About This Document 3

1.1 About This Document 3
1.2 Related Documents 3
1.3 Document history 3
1.4 Conventions 4

2 Description 5

2.1 Intended Use 5

3 Installation 6

3.1 Connector Pinning 7
3.2 Cabling 8

4 Configuration 9

4.1 Easy Config 10
4.2 Network Settings 12
4.3 WLAN Settings 13
4.4 Bluetooth Settings 15
4.5 Firmware Update 16
4.6 AT Commands 16
4.7 System Settings 17
4.8 Factory Reset 18
4.9 Configuration Examples 20

A Technical Data 23

This page intentionally left blank

1 About This Document

1.1 About This Document

This manual describes how to install and configure Anybus Wireless Bolt.

For additional related documentation and file downloads, please visit the support website at www.anybus.com/support.

1.2 Related Documents

Related documents

Document	Author
Anybus Wireless Bolt Installation Guide	HMS
Anybus Wireless Bolt AT Commands Reference	HMS

1.3 Document history

Revision list

Version	Date	Description
1.00	2016-09-15	First release

Summary of changes in this version

Change	Where (section no.)

1.4 Conventions

Unordered (bulleted) lists are used for:

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

Ordered (numbered or alphabetized) lists are used for instructions that must be carried out in sequence:

1. First do this,
2. Then open this dialog, and
   a. set this option...
   b. ...and then this one.

Bold typeface indicates interactive parts such as connectors and switches on the hardware, or menus and buttons in a graphical user interface.

```
Monospaced text is used to indicate program code and other
kinds of data input/output such as configuration scripts.
```

This is a cross-reference within this document: *Conventions, p. 4*

This is an external link (URL): www.hms-networks.com

This is additional information which may facilitate installation and/or operation.

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

Caution
This instruction must be followed to avoid a risk of personal injury.

WARNING
This instruction must be followed to avoid a risk of death or serious injury.

2 Description

Anybus Wireless Bolt combines Bluetooth® Classic/Low Energy and 2.4 GHz/5 Ghz WLAN connectivity with Ethernet networking and optionally with serial RS-232/485 or CAN.

Bluetooth and WLAN can be used simultaneously. The Ethernet port can be used at the same time as one of the serial or CAN ports.

The WLAN interface can use either the 2.4 GHz or the 5 GHz channel band, not both at the same time.

The unit can be configured as a client or access point for both Bluetooth and WLAN. It contains an internal DHCP server for dynamic IP addressing on a local network.

2.1 Intended Use

Typical applications for Anybus Wireless Bolt include:

- Adding wireless cloud connectivity to industrial devices
- Accessing devices from a laptop, smartphone or tablet
- Ethernet cable replacement between devices

Anybus Wireless Bolt can only handle a limited number of connected devices and is not intended for bridging large networks. Please visit the Anybus website at www.anybus.com for more information about our complete range of wireless networking solutions.

3 Installation

Anybus Wireless Bolt should be mounted vertically (logo facing upwards) for best performance due to the characteristics of the internal antenna.

For optimal reception, wireless devices should be placed with a line of sight between them clear of obstructions. A minimum distance of 50 cm between the devices should be observed to avoid interference.

Make sure that you have all the necessary information about the capabilities and restrictions of your local network environment before installing the Anybus Wireless Bolt. Contact your network administrator if in doubt.

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

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

Mechanical Installation

Anybus Wireless Bolt is intended to be mounted on top of a machine or cabinet through an M50 (50.5 mm) hole using the included sealing ring and nut.

Tightening torque: 5 Nm ±10 %

Make sure that the sealing ring is correctly placed in the circular groove in the top part of the housing before tightening the nut.

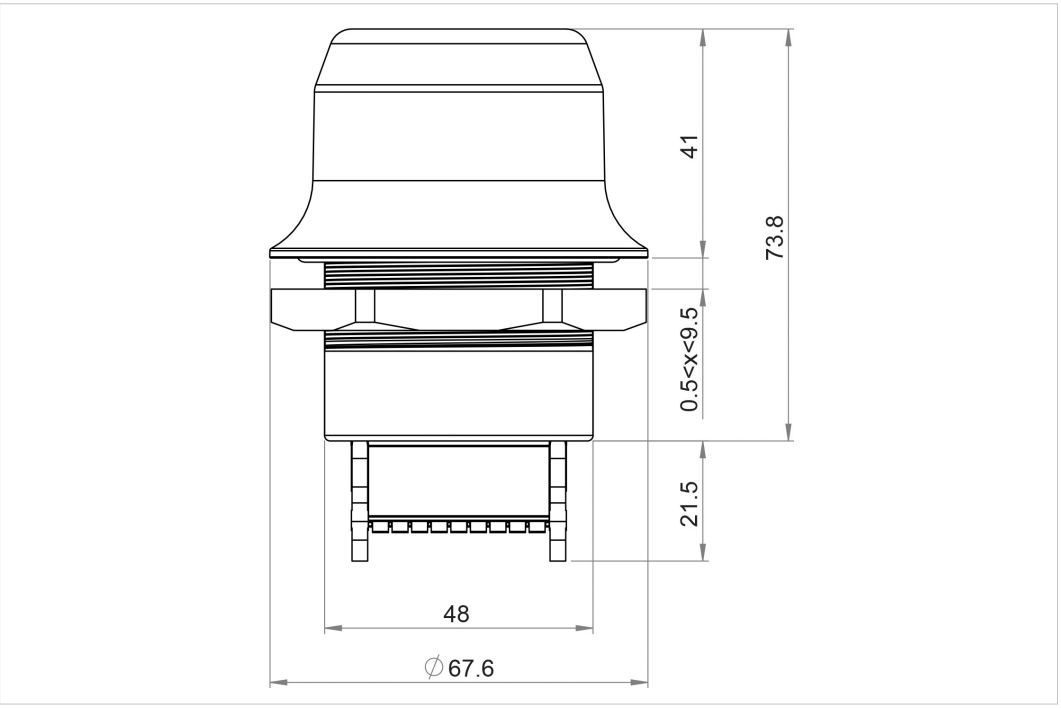


Fig. 1 Installation drawing

All measurements are in mm.

3.1 Connector Pinning

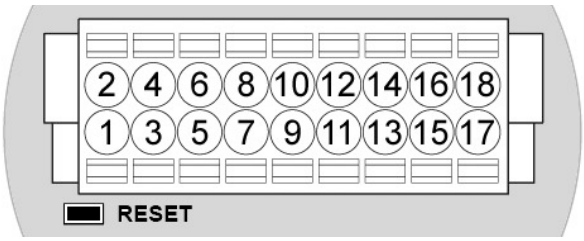


Fig. 2 Connector

For correct pin identification, observe the location of the **RESET** button when the connector is attached to the Wireless Bolt. Pin 1 is the pin closest to the button.

Pin	Name	Description
1	VIN	Power 9–30 VDC
2	GND	Power Ground
3	DI	Digital input (9–30 VDC)
4	DI_GND	Digital input ground
5	ETN_RD+	Ethernet receive + (white/orange)
6	ETN_RD-	Ethernet receive - (orange)
7	ETN_TD-	Ethernet transmit - (green)
8	ETN_TD+	Ethernet transmit + (white/green)
9	RS485_B	RS-485 B Line
10	FE/Shield	Functional Earth/Functional Earth and Shield for serial interface
11	RS232_TXD	RS-232 Transmit
12	RS485_A/RS232_RXD	RS-485 A Line or RS-232 Receive
13	RS232_RTS	RS-232 Request To Send
14	RS232_CTS	RS-232 Clear To Send
15	ISO_5V	Isolated 5 V for serial interface
16	ISO_GND	Isolated Ground for serial interface
17	CAN_L	CAN Low
18	CAN_H	CAN High

- RS-232 and RS-485 cannot be used at the same time.
- Use termination for RS-485 and CAN when needed.

> **!** If using a shielded Ethernet cable the shield must be unconnected.

3.2 Cabling

To make an Ethernet connector cable for the Anybus Wireless Bolt:

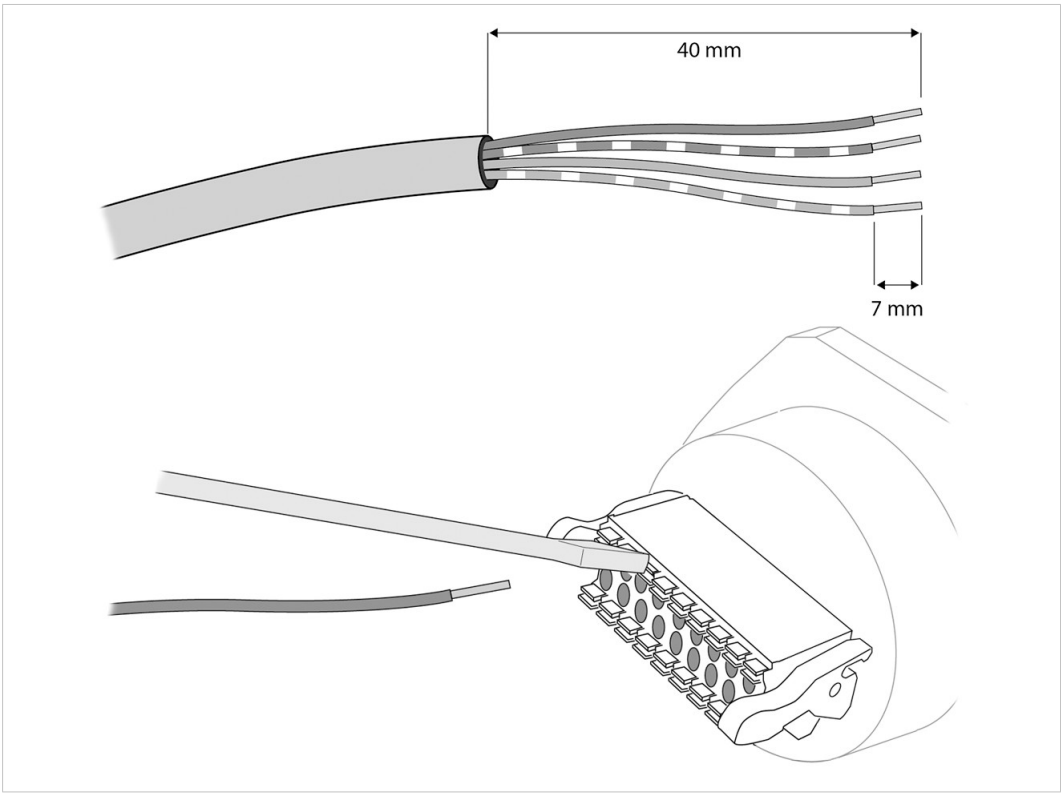


Fig. 3 Ethernet cable

1. Cut off one of the connectors on a standard Cat5e or Cat6 Ethernet cable.
2. Strip off about 40 mm (1½ inch) of the cable jacket and untwist the orange, orange/white, green and green/white wires. The other wires will not be used.
3. Strip off about 7 mm (¼ inch) of the isolation on each wire.
4. Push the pin spring release next to each socket on the connector and insert the correct wire end according to *Connector Pinning, p. 7*.

Connect the wires from the power supply to the connector in the same way as the Ethernet wiring. Make sure that polarity is not reversed.

4 Configuration

Anybus Wireless Bolt is normally configured through the built-in web interface, either by setting individual parameters or by using a pre-configured **Easy Config** mode.

The web interface is accessed by pointing a web browser to the IP address of the internal web server in Wireless Bolt. The default address is **192.168.0.99**.

The first page shows an overview of the current settings. For details about each configuration section, select the respective section from the menu.

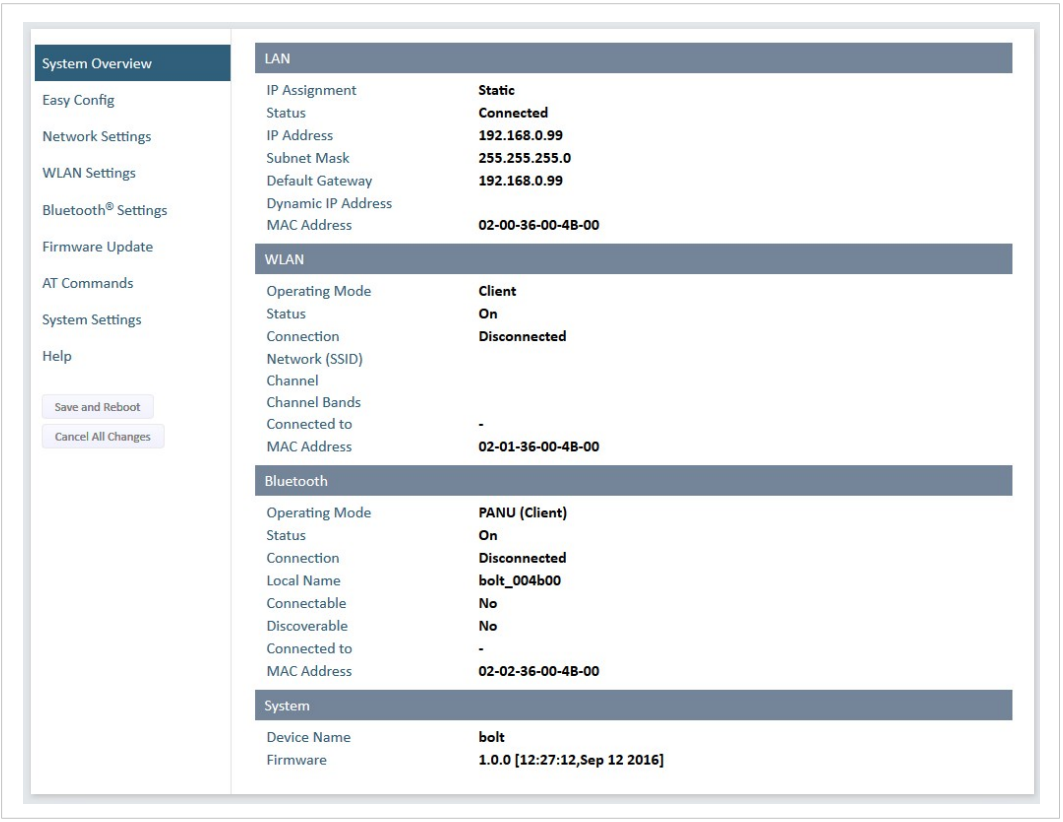


Fig. 4 System Overview

If the Anybus Wireless Bolt needs to be restarted for a parameter change to come into effect, the **Save and Reboot** button will become enabled. To return to the current configuration without saving, click on **Cancel All Changes**.

> **!** The web interface is designed for the latest versions of Internet Explorer, Chrome, Firefox and Safari. Other browsers may not be supported.

Advanced Configuration

Advanced configuration can be carried out by entering AT (Hayes) command strings directly into the **AT Commands** tab in the web interface, or using a terminal emulator over a Telnet connection to port 8080. A reference manual describing the supported AT commands can be downloaded from www.anybus.com/support.

See also *AT Commands, p. 16*.

4.1 Easy Config

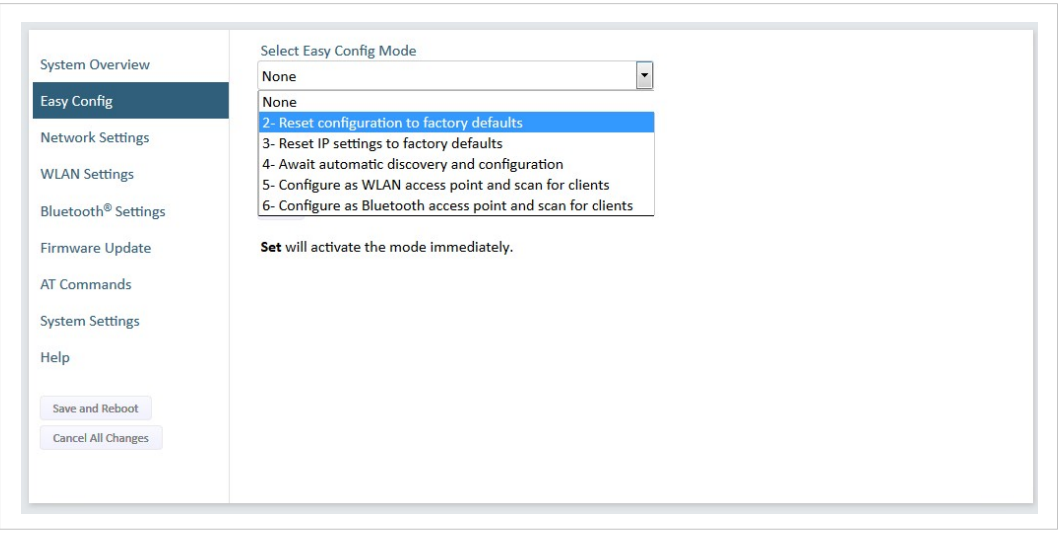


Fig. 5 Easy Config page

Easy Config modes can be used for automatic configuration of the Anybus Wireless Bolt.

Modes 2 and 3 are used to recall factory settings. Modes 4, 5 and 6 can be used in combination to automatically set up a WLAN or Bluetooth connection between Wireless Bolt devices.

To activate an Easy Config mode, select it from the dropdown menu and click on **Set**.

See also *Configuration Examples, p. 20*.

Easy Config Modes

Mode 2 - Reset configuration to factory defaults

Resets the configuration to the factory defaults and reboots the device.

See also *Factory Reset, p. 18*.

Mode 3 - Reset IP settings to factory defaults

Resets the IP settings to their factory defaults, clears the table holding the IP addresses of associated WLAN/Bluetooth clients, and reboots the device.

> **!** When resetting a device to the factory defaults, its IP address will be reset to 192.168.0.99. Associated devices that were connected using Easy Config may also have to be reconfigured to avoid IP address conflicts.

Mode 4 - Await automatic discovery and configuration

The device will wait for an attempt from another device set in Mode 5 or 6 to connect. The connecting device will send a configuration to the device set in Mode 4, which will then apply the received settings and reboot.

The mode will time out after 120 seconds. If no connection has been established within the timeout period the device will return to its initial state.

Mode 5 - Configure as WLAN access point and scan for clients

Scan for devices set in Mode 4. If at least one such device is discovered, the scanning device will configure itself as a WLAN access point, send a configuration to the other devices, and reboot. The other devices will automatically reboot and connect to the access point as clients.

The mode will time out after scanning for 120 seconds. If no connection has been established within the timeout period the device will return to its initial state.

The access point will automatically assign IP addresses within its own Ethernet subnet range to the clients. See also *Network Settings, p. 12*.

Mode 6 - Configure as Bluetooth access point and scan for clients

Same as Mode 5 but using Bluetooth. The device will be configured as a Bluetooth NAP.

Notes on using Easy Config modes 4–6:

- The devices will be unavailable on the network until the configuration attempt has succeeded or the mode times out.
- The IP address of a client may be changed by the configuration from the access point. Active browser sessions could therefore be lost.
- The devices will always use Bluetooth during the scanning phase. After that they will use either Bluetooth or WLAN depending on the selected mode.

4.2 Network Settings

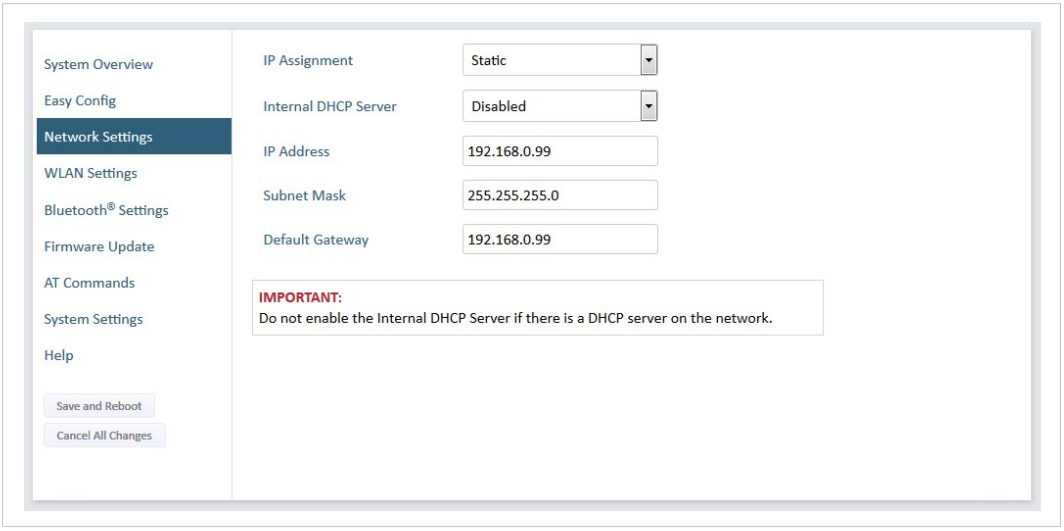


Fig. 6 Network Settings page

IP Assignment	Select static or dynamic IP addressing (DHCP) for the Wireless Bolt.
Internal DHCP Server	Activates an internal DHCP server which will assign IP addresses within the current subnet to devices that use DHCP. **Do not enable this option if there is already a DHCP server on the network!**
IP Address	Static IP address for the Wireless Bolt
Subnet Mask	Subnet mask when using static IP
Default Gateway	Default gateway when using static IP

When the IP address is changed the browser should automatically be redirected to the new address after clicking on **Save and Reboot**. This function may not be supported by all browsers.

4.3 WLAN Settings

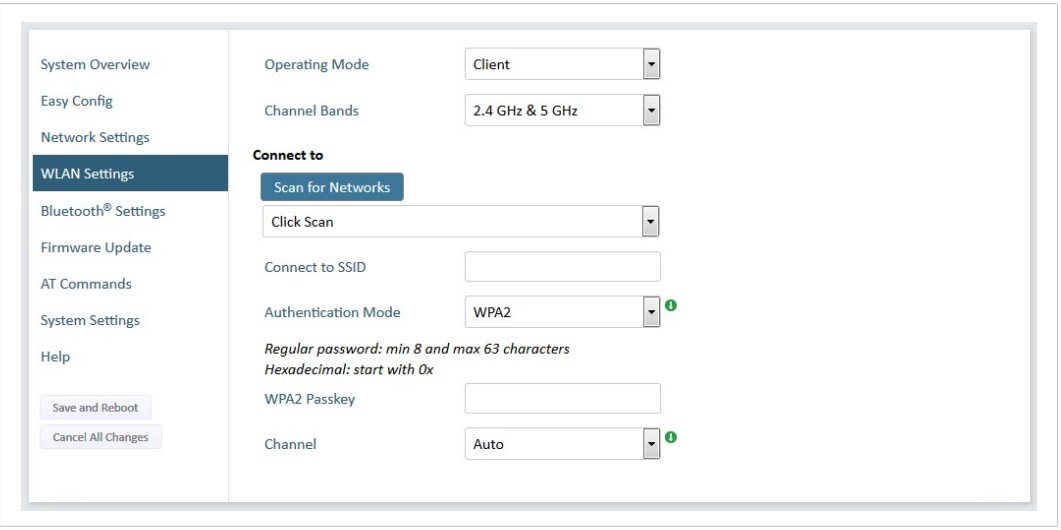


Fig. 7 WLAN Settings — Client

Operating Mode	Choose if the Wireless Bolt should operate as a WLAN Client or Access Point. If Access Point is selected, additional parameters will be visible.
Channel Bands	Choose to scan for networks on either the 2.4 GHz or the 5 GHz channel band, or both. The unit must be rebooted to enable the new setting. Please note that although the Wireless Bolt can scan on both channel bands, it can only operate on one band at a time.
Scan for Networks	Scans the currently active frequency band for discoverable WLAN networks. To connect to a network, select it from the dropdown menu when the scan has completed.
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** = No encryption or authentication **WPA2** = WPA2 PSK authentication with AES/CCMP encryption Other authentication and encryption modes can be selected using AT commands. See the Anybus Wireless Bolt AT Commands Reference.
WPA2 Passkey	Enter the WPA2 passkey for the network.
Channel	Select a specific channel to use when scanning for networks. Which channels are available depend on the **Channel Bands** setting. **Auto** = all channels will be scanned (default).

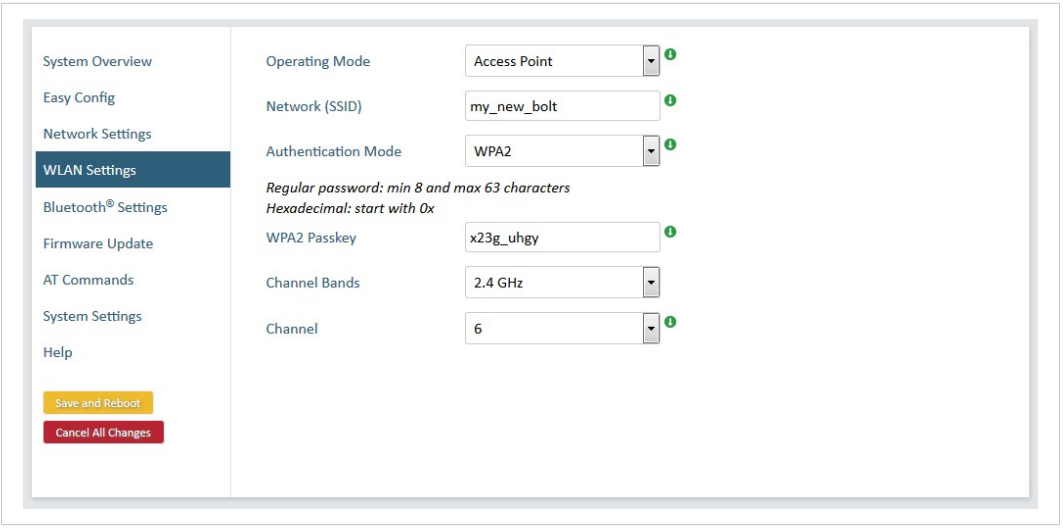


Fig. 8 WLAN Settings — Access Point

Network (SSID)	Enter an SSID (network name) for the Wireless Bolt. If left blank, the unit will use the default SSID **bolt_xxyyzz**, where “xxyyzz” are the last part of the MAC ID.
Authentication Mode	Select the authentication/encryption mode to use for the access point. **Open** = No encryption or authentication **WPA2** = WPA2 PSK authentication with AES/CCMP encryption
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. Hexadecimal passwords must start with `0x` and be **exactly** 64 characters. See also the example passwords below.
Channel Bands, Channel	Select the WLAN channel band and channel to use for the access point.

Password examples

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

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

Example of hexadecimal password:
`0x000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f`

> **!** Do not use the example passwords above in a real installation.

4.4 Bluetooth Settings

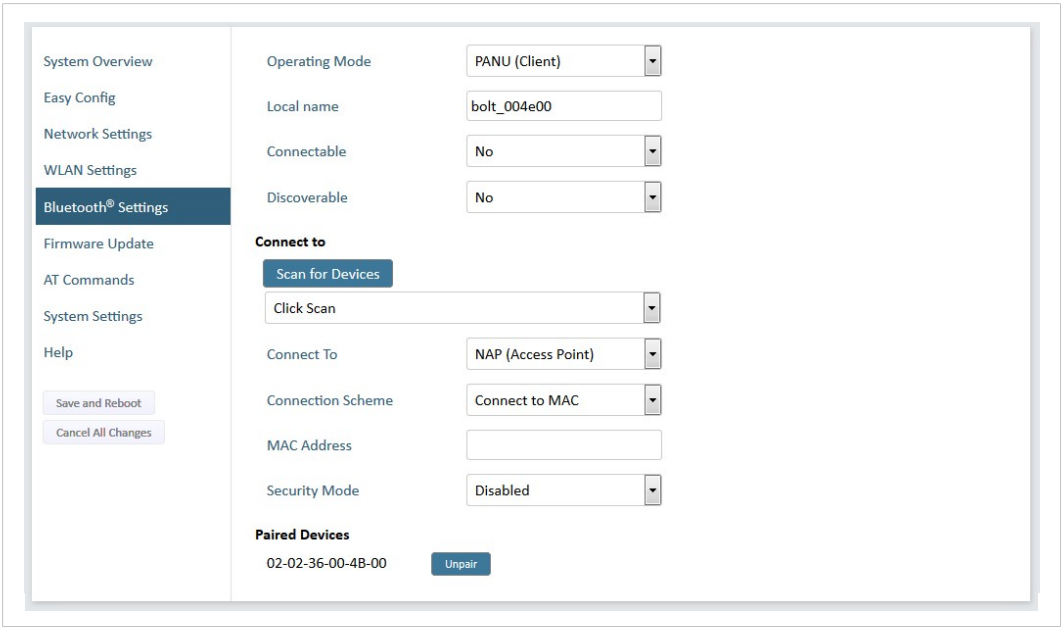


Fig. 9 Bluetooth Settings — PANU (Client)

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	The name identifying the unit to other Bluetooth devices. The default name is **bolt_xxyyzz**, where “xxyyzz” are the last part of the MAC ID.
Connectable	Enable to make the unit accept connections initiated by other Bluetooth devices.
Discoverable	Enable to make the unit visible to other Bluetooth devices.
Security Mode	**Disabled** = No encryption or authentication. **PIN** = Encrypted connection with PIN code security. This mode only works when connecting to another Wireless Bolt. PIN codes must consist of 4 to 6 digits. **Just Works** = Encrypted connection without PIN code.
Paired Devices	Lists the currently connected Bluetooth devices.

PANU mode only

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 or name when connecting manually.

NAP mode only

List Nearby Devices	Scans the network and lists discoverable Bluetooth devices. Pairing cannot be initiated in NAP mode.

4.5 Firmware Update

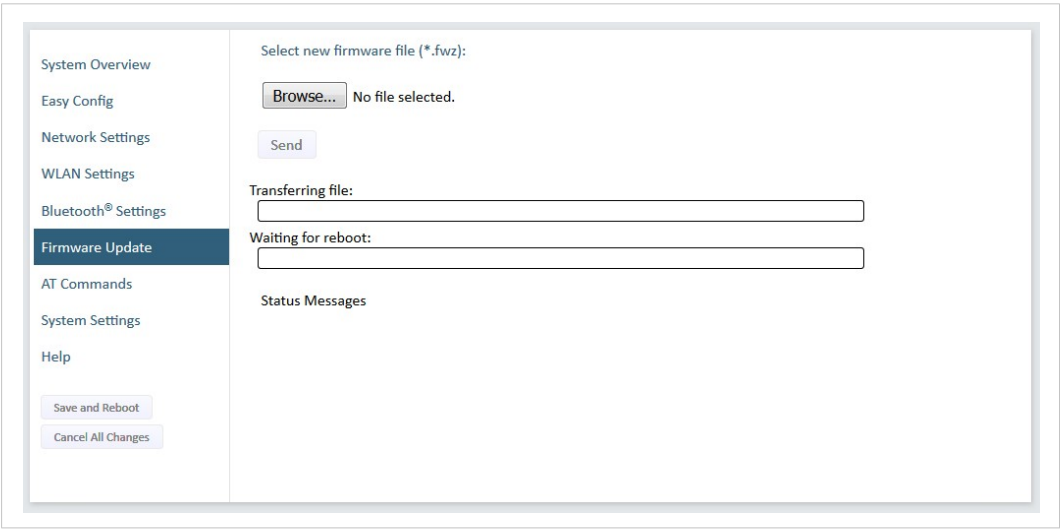


Fig. 10 Firmware Update

Click on **Browse** to select a firmware file, then click on **Send** to download it to the Wireless Bolt.

Both progress bars will turn green when the firmware update is completed. The unit will then reboot automatically.

4.6 AT Commands

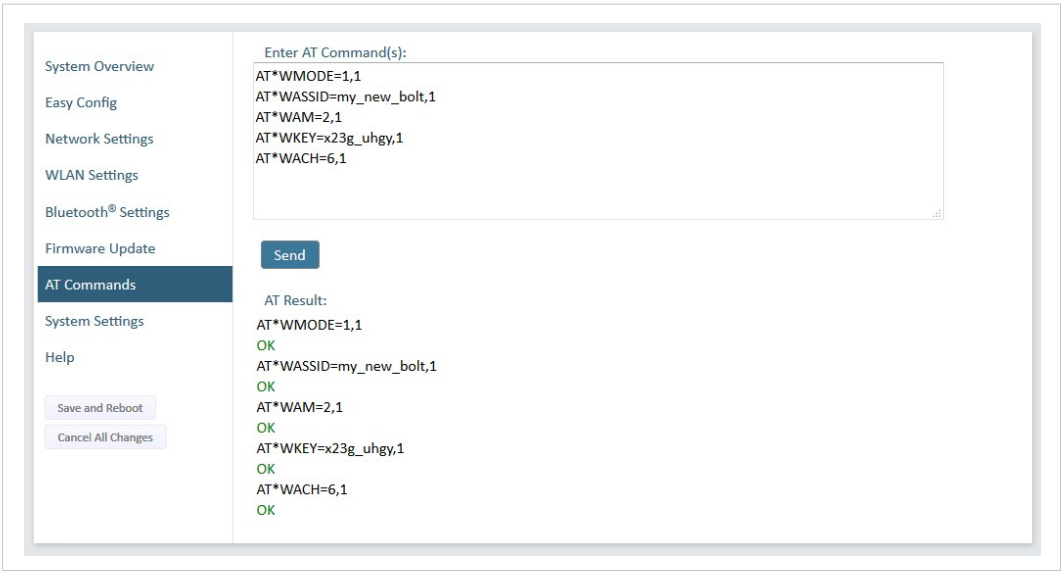


Fig. 11 AT Commands

AT commands can be used for setting parameters that are not available in the web interface, and for batch configuration using command scripts.

Enter or paste the commands into the text box, then click on **Send**. The result codes will be displayed below the text box.

A reference manual describing all supported AT commands for Anybus Wireless Bolt can be downloaded from www.anybus.com/support.

4.7 System Settings

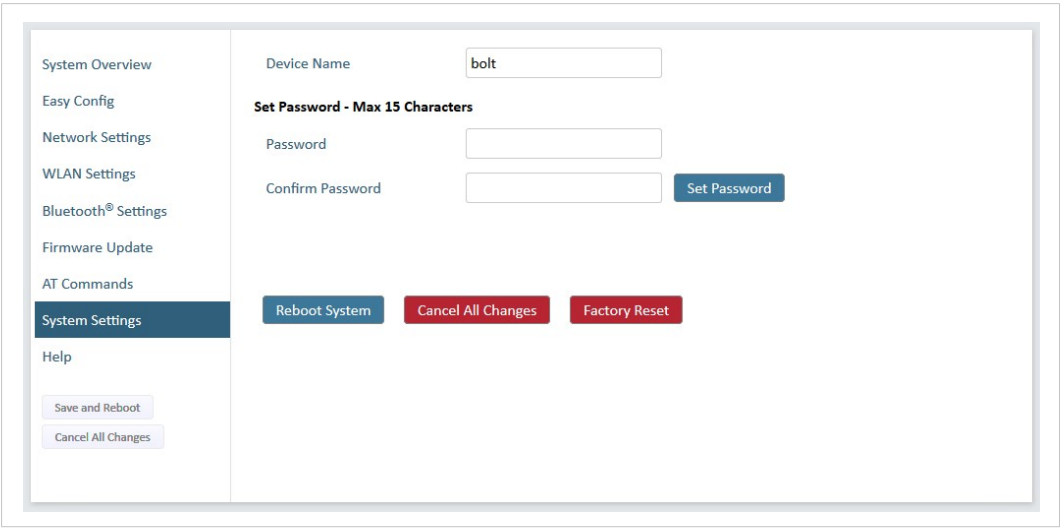


Fig. 12 System Settings

Device Name	Enter a descriptive name for the Wireless Bolt.
Password	Enter a password for accessing the web interface.
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.

> **!** Setting a secure password for the unit is strongly recommended.

4.8 Factory Reset

Anybus Wireless Bolt can be reset to the factory default settings using either of the following methods:

- Press and hold the **Reset Button** for >10 seconds and then release it
- Execute **Easy Config Mode 2**
- Issue the AT command **AT&F** and reboot

4.8.1 Factory Default Settings

Network Settings

IP Assignment	Static
IP Address	192.168.0.99
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.99

WLAN Settings

Operating Mode	Client
Channel Bands	2.4 GHz & 5 GHz
Authentication Mode	Open
Channel	Auto

Bluetooth Settings

Operating Mode	PANU (Client)
Local Name	[generated from MAC address]
Security Mode	Disabled

System Settings

Password	[empty]

> **!** Setting a secure password for the unit is strongly recommended.

4.8.2 Reset Button

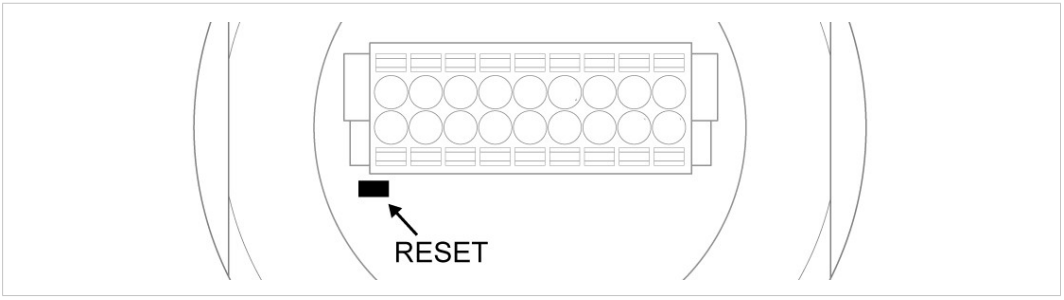


Fig. 13 Reset button

The reset button is located on the bottom of the unit next to the connector.

- Press and hold the button for >10 seconds and then release it to reset to the factory default settings when the unit is powered on.
- Press and hold the button during startup to enter *Recovery Mode*.

Recovery Mode

If the web interface cannot be accessed, the unit may be reset by starting in Recovery Mode and reinstalling the firmware using Anybus Firmware Manager II.

For instructions, please refer to the wizard in Anybus Firmware Manager II.

> **!** Firmware updates should normally be carried out through the web interface. Recovery Mode should only be used if the Wireless Bolt is unresponsive and the web interface cannot be accessed.

4.9 Configuration Examples

The following examples require a basic understanding of how to install Anybus Wireless Bolt and how to access and use the web interface. Please read the *Installation* and *Configuration* sections before you continue.

- All the examples start out from the factory default settings.
- Settings not mentioned in the examples should normally be left at their default values.
- The computer accessing the web interface must be in the same subnet as the Wireless Bolt being configured.

4.9.1 Setting up an Ethernet network bridge with Easy Config

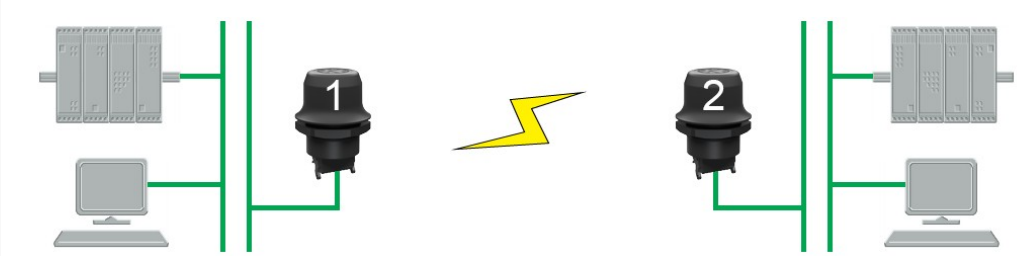


Fig. 14 Setting up a network bridge with Easy Config

This example describes how to connect two Ethernet network segments over WLAN or Bluetooth using two Wireless Bolts.

1. On Wireless Bolt 1, execute **Easy Config Mode 4**. This unit will now be discoverable and open for automatic configuration.

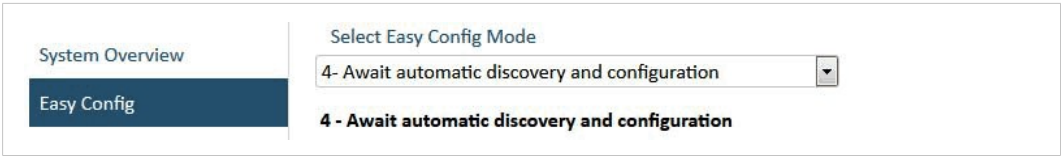


Fig. 15

2. On Wireless Bolt 2, execute either **Easy Config Mode 5** for WLAN, or **6** for Bluetooth. This unit should now automatically discover and configure Wireless Bolt 1 as a WLAN or Bluetooth client.

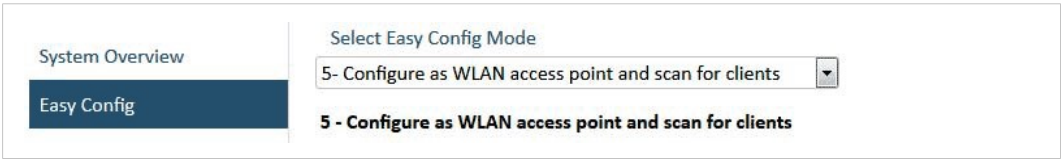


Fig. 16

If no connection is established within 120 seconds the Easy Config modes will be aborted and the units will restart in the previous state.

4.9.2 Accessing a PLC from a handheld device using WLAN

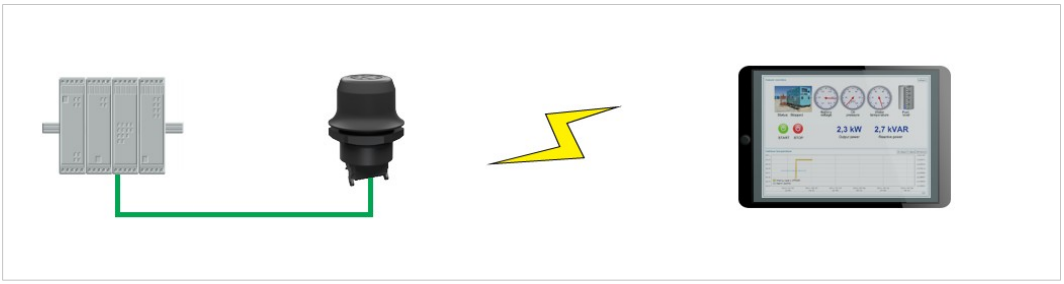


Fig. 17 Accessing a PLC from a handheld device using WLAN

This example describes how to access the web interface of a PLC from a tablet or smartphone using WLAN.

Refer to the documentation for the PLC and the handheld device on how to configure their network settings.

A: The PLC or network has an active DHCP server

1. **Network Settings:** Select **IP Assignment**: **Dynamic (DHCP)** and continue to step 3 below.

B: The PLC has a static IP address, no DHCP server on the network

1. Make sure that the IP addresses of the PLC and the Wireless Bolt are within the same Ethernet subnet.
2. **Network Settings:** Select **IP Assignment**: **Static** and enable **Internal DHCP Server**.
3. **WLAN Settings:** Select **Operating Mode** – **Access Point** and enter a unique SSID (network name) for the unit.

   Select an Authentication Mode and a WLAN channel if required by your network environment, otherwise leave them at the default settings.
4. Click on **Save and Reboot** to restart the Wireless Bolt with the new settings.
5. In the WLAN configuration of the handheld device, connect to the SSID of the Wireless Bolt.

   You should now be able access the web interface of the PLC by entering its IP address in the web browser on the handheld device.

> **!** Do not enable Internal DHCP Server if there is already a DHCP server on the network.

This page intentionally left blank

A Technical Data

General Specifications

Wired Interface Type	Ethernet	Serial RS-232/485 + Ethernet	CAN + Ethernet
Order code	AWB2000	AWB2010	AWB2020
Range	Up to 100 meters		
Antenna	Built-in		
Operating temperature	-40 to +65 °C		
Weight	81 g		
Housing	Plastic (PBT glass-reinforced/PC-ABS)		
IP class	IP67 for top (outside of host), IP21 for bottom (inside of host)		
Dimensions	Height: 70 mm (95 mm incl. connector, 41 mm outside of host) Diameter: 70 mm		
Mounting	M50 screw and nut (50.5 mm hole required)		
Connector	Included plug connector (2 x 9 pin 3.5 mm Phoenix DFMC 1.5/9-ST-3.5 push-in spring connection)		
Power supply	9–30 VDC (-5% +20%) Cranking 12 V (ISO 7637-2:2011 pulse 4) Polarity reversal protection		
Power consumption	0.7 W (idle) – 1.7 W (max)		
Browser support	Internet Explorer, Firefox, Chrome, Safari (latest stable versions)		
Configuration	Built-in web interface / Easy Config Modes / AT commands		
Vibration compatibility	Sinosodial vibration test according to IEC 60068-2-6:2007 and with extra severities; – Number of axes: 3 mutually perpendicular (X:Y:Z), – Duration: 10 sweep cycles in each axes, – Velocity: 1 oct/min, – Mode: in operation, – Frequency: 5–500 Hz, – Displacement ±3.5 mm, – Acceleration: 2 G. Shock test according to IEC 60068-2-27:2008 and with extra severities; – Wave shape: half sine, – Number of shocks: ±3 in each axes, – Mode: In operation, – Axes ± X,Y,Z, – Acceleration: 30 m/s^2 , – Duration: 11 ms		
Humidity compatibility	EN 600068-2-78: Damp heat, +40 °C, 93 % humidity for 4 days		
Certifications	Pending (see Anybus Wireless Bolt Compliance Sheet)		

Host Communication

Ethernet interface	10/100BASE-T with automatic MDI/MDIX cross-over detection IP, TCP, UDP, HTTP, LLDP, ARP, DHCP Client/Server, DNS support PROFINET IO, EtherNet/IP, Modbus-TCP
Serial interface	Isolated RS-232/485 (max. 1 Mbit/s)
CAN interface	Isolated CAN (max. 1 Mbit/s)
Digital input	Max 3 m signal cable length

WLAN Specifications

Wireless standards	WLAN 802.11a/b/g/d/e/i/h
Operation modes	Access Point or Client
2.4 GHz channels	1–11
5 GHz channels	36–48 (U-NII-1), 52–64 (U-NII-2), 100–140 (U-NII-2e)
RF output power	16 dBm
Max number of clients	7 (for access point)
Power consumption	54 mA @ 24 VDC (WLAN interface only)
Net data throughput	Up to 20 Mbit/s
Authentication	WPA-PSK, LEAP, PEAP
Encryption	WEP64/128, WPA, WPA2, TKIP, AES/CCMP

Bluetooth Specifications

Core specification	4.0
Wireless profiles	PAN (PANU & NAP)
Operation modes	Access Point or Client
RF output power	10 dBm
Max number of clients	7 (for access point)
Power consumption	36 mA @ 24 VDC (Bluetooth interface only)
Net data troughput	Up to 1 Mbit/s
Security	Authentication & Authorization, Encryption & Data Protection, Privacy & Confidentiality, NIST Compliant, FIPS Approved

This page intentionally left blank

HMS Industrial Networks AB
Box 4126
300 04 Halmstad, Sweden

info@hms.se

© 2016 HMS Industrial Networks AB
SCM-1202-007 1.0.1956 / 2016-09-15 15:32